

Ultima modifica: 29.07.2026

PDF creato il: 06.10.2026



COMMENTARIO ONLINE
IL COMMENTARIO GIURIDICO
IN OPEN ACCESS

INDICE

Art. 1 CCC (Convenzione sulla cibercriminalità [Cybercrime Convention])	5
Art. 2 CCC (Convenzione sulla cibercriminalità [Cybercrime Convention]) .	29
Art. 3 CCC (Convenzione sulla cibercriminalità [Cybercrime Convention]) .	43
Art. 4 CCC (Convenzione sulla cibercriminalità [Cybercrime Convention]) .	57
Art. 5 CCC (Convenzione sulla cibercriminalità [Cybercrime Convention])..	67
Art. 6 CCC (Convenzione sulla cibercriminalità [Cybercrime Convention]) .	79
Art. 7 CCC (Convenzione sulla cibercriminalità [Cybercrime Convention])..	93
Art. 8 CCC (Convenzione sulla cibercriminalità [Cybercrime Convention])	103
Art. 9 CCC (Convenzione sulla cibercriminalità [Cybercrime Convention])	113
Art. 11 CCC (Convenzione sulla cibercriminalità [Cybercrime Convention])	127
Art. 12 CCC (Convenzione sulla cibercriminalità [Cybercrime Convention])	133
Art. 16 CCC (Convenzione sulla cibercriminalità [Cybercrime Convention])	149
Art. 18 CCC (Convenzione sulla cibercriminalità [Cybercrime Convention])	163
Art. 25 CCC (Convenzione sulla cibercriminalità [Cybercrime Convention])	181
Art. 27 CCC (Convenzione sulla cibercriminalità [Cybercrime Convention])	193
Art. 28 CCC (Convenzione sulla cibercriminalità [Cybercrime Convention])	211
Art. 29 CCC (Convenzione sulla cibercriminalità [Cybercrime Convention])	219
Art. 32 CCC (Convenzione sulla cibercriminalità [Cybercrime Convention])	239
Art. 33 CCC (Convenzione sulla cibercriminalità [Cybercrime Convention])	283

Art. 34 CCC (Convenzione sulla cibercriminalità [Cybercrime Convention])
..... 299

ATTENZIONE: Questa versione del commentario è una traduzione automatica dell'originale. Il commentario originale è in francese. La traduzione è stata effettuata con www.deepl.com. Solo la versione originale fa fede. La forma tradotta del commentario non può essere citata

COMMENTO SU

Art. 1 CCC (Convenzione sulla cibercriminalità [Cybercrime Convention])

Un commentario di Jérémie Müller

CITAZIONE SUGGERITA

Jérémie Müller, Commentario all'art. 1 CCC, in: Damian K. Graf (a cura di), Commentario online alla Convenzione sulla cibercriminalità [Cybercrime Convention]

Breve citazione: OK-Müller, art. 1 CCC N. XXX.

Capitolo I: Terminologia

Art. 1 Definizioni

Ai sensi della presente Convenzione, s'intende per:

- a. sistema informatico: qualsiasi apparecchiatura o gruppo di apparecchiature interconnesse o collegate, una o più delle quali effettuano l'elaborazione automatica di dati in base a un programma;
- b. dati informatici: qualunque presentazione di fatti, informazioni o concetti in una forma che si presta a elaborazione informatica, inclusi i

programmi che permettono a un sistema informatico di svolgere una funzione;

c. fornitore di servizi:

i. qualunque entità pubblica o privata che fornisce agli utenti dei propri servizi la possibilità di comunicare attraverso un sistema informatico, e

ii. qualunque altra entità che elabora o memorizza dati informatici per conto di tale servizio di comunicazione o per gli utenti di questo servizio;

d. dati relativi al traffico informatico: tutti i dati relativi a una comunicazione che passa attraverso un sistema informatico, prodotti da quest'ultimo in quanto elemento della catena di comunicazione e indicanti l'origine, la destinazione, il percorso, l'ora, la data, la dimensione e la durata della comunicazione o il tipo di servizio utilizzato per la comunicazione.

STRUTTURA

I. Considerazioni generali.....	8
II. Sistema informatico (Let. A).....	8
A. Un dispositivo	9
B. Un programma	11
C. Il trattamento automatico dei dati	11
D. Prospettive	12
1. La dematerializzazione dei sistemi informatici	12
2. L'Internet delle cose (IoT).....	13
3. L'intelligenza artificiale.....	14
III. Dati informatici (lett. b).....	15
A. La forma dei dati	15
B. I tipi di dati	16
C. I programmi	17
D. Prospettive	18
E. Excursus: la distinzione tra dati relativi all'abbonato, dati relativi al traffico e dati di contenuto nel diritto penale svizzero.....	18
1. I dati relativi all'abbonato	19
2. I dati relativi al traffico (o dati secondari)	19
3. I dati di contenuto	20
IV. Fornitore di servizi (lett. c)	21
A. I fornitori di accesso.....	21
B. I fornitori di spazio di archiviazione o di contenuti	23
C. Prospettive	24
V. Dati relativi al traffico (lett. d).....	25
Bibliografia	27
I materiali.....	27

I. CONSIDERAZIONI GENERALI

- 1 La Convenzione sulla criminalità informatica inizia fornendo, all'articolo 1, quattro definizioni dei concetti fondamentali a cui fanno riferimento i vari articoli successivi. I redattori della Convenzione hanno certamente precisato nella loro Relazione esplicativa che le Parti non sarebbero tenute a riprodurre alla lettera, nelle loro leggi interne, i quattro concetti definiti all'art. 1 della Convenzione. Hanno tuttavia precisato che le leggi nazionali devono disciplinare tali concetti in modo compatibile con i principi della Convenzione e offrire un quadro equivalente per la sua attuazione. L'importanza di queste definizioni appare quindi chiara: mettere tutte le Parti su un piano di parità per garantire che facciano riferimento agli stessi concetti. Ciò consente in particolare di **evitare controversie**, ad esempio che una Parte si rifiuti di applicare determinate disposizioni con la motivazione di interpretare un concetto in modo diverso rispetto a un'altra Parte.
- 2 I redattori della Convenzione erano evidentemente **consapevoli della rapida evoluzione** dell'informatica. È senza dubbio per questo motivo che hanno deciso di formulare le definizioni dell'art. 1 CCC nel modo più neutro possibile dal punto di vista tecnologico, limitandosi alla descrizione funzionale di ciascun concetto. Questa strategia ha dato i suoi frutti, poiché, venticinque anni dopo, tali definizioni rimangono pertinenti nonostante la notevole evoluzione tecnologica avvenuta nel corso di questo periodo.

II. SISTEMA INFORMATICO (LET. A)

- 3 La definizione adottata dagli autori della Convenzione sulla criminalità informatica si compone di **tre aspetti**. Essa presuppone, in primo luogo, l'esistenza di un dispositivo. Quest'ultimo può essere isolato o collegato in rete. La definizione comprende quindi sia il personal computer che gli ambienti informatici interconnessi. Il secondo elemento risiede nella presenza di un programma. È quindi necessario che il dispositivo funzioni sulla base di istruzioni prestabilite. Il dispositivo non può essere puramente meccanico. Un carillon o un orologio non sono quindi sistemi informatici. Infine, il trattamento dei dati deve avvenire in modo automatico. Non è sufficiente che il dispositivo si limiti a un'archiviazione passiva dei dati, ma deve eseguire automaticamente un processo di trasformazione di tali dati. Una macchina

fotografica, un dittafono o una chiavetta USB non sono quindi sistemi informatici.

Nelle sue linee guida, il Comitato della Convenzione sulla criminalità 4 informatica ha precisato che la definizione di «sistema informatico» include, ad esempio, i **moderni telefoni cellulari** che sono multifunzionali e tra le loro funzioni hanno la capacità di produrre, elaborare e trasmettere dati, quali l'accesso a Internet, l'invio di e-mail, la trasmissione di allegati, il download di contenuti o documenti. Lo stesso vale per i **personal digital assistant**, con o senza funzionalità wireless, che producono, elaborano e trasmettono anch'essi dati.

La definizione adottata considera volutamente il sistema informatico dal 5 punto di vista della sua **funzionalità**, e non della sua forma. Questo approccio le conferisce una flessibilità sufficiente per evolversi nel tempo e includere tecnologie che nel 2001 non esistevano ancora, quali gli *smartphone*, l'Internet delle cose (*IoT*) o il *cloud computing*.

A. Un dispositivo

L'informatica si basa fundamentalmente sull'elaborazione dei dati. 6 Quest'ultimo concetto sarà approfondito più avanti al punto III. A questo stadio, i dati possono essere definiti come informazioni digitali immateriali. Per poter essere elaborate, tali informazioni richiedono tuttavia un **insieme di componenti hardware** che ne consentano sia l'elaborazione che l'archiviazione.

Sebbene non costituisca l'elemento più importante del sistema informatico, la 7 **scheda madre** ne rappresenta comunque la struttura portante. Si tratta di una grande scheda elettronica che funge da supporto per tutti i componenti del sistema. L'elemento veramente centrale del sistema informatico è il **processore**. Esso rappresenta il cuore del sistema, in quanto elabora tutte le istruzioni e le richieste che gli pervengono dai vari componenti. Una volta elaborati i dati, il processore deve poterli memorizzare temporaneamente da qualche parte, poiché non è dotato di memoria propria. I dati vengono quindi memorizzati temporaneamente nella **memoria RAM**. Questa memoria, tuttavia, può conservare i dati solo quando il sistema informatico è acceso. Quando si spegne, tutti i dati contenuti in questa memoria vanno persi. È quindi necessario prevedere una memorizzazione duratura di questi dati su

un dispositivo appropriato, come un disco rigido, un disco rigido esterno, una chiavetta USB, un DVD, ecc.

- 8 Gli ultimi componenti indispensabili al funzionamento del sistema informatico sono le **periferiche**. Le periferiche di input consentono l'immissione dei dati nel sistema, come il mouse, la tastiera o lo scanner. A queste si contrappongono le periferiche di output che assicurano la restituzione dei dati elaborati dal sistema, come lo schermo, la stampante o il masterizzatore DVD. Tutti questi elementi materiali sono chiamati *hardware* e formano un dispositivo.
- 9 Sarebbe tuttavia riduttivo pensare che tutti i componenti che formano il dispositivo debbano necessariamente trovarsi in **un unico luogo** in modo compatto, poiché ciò equivarrebbe a limitare il concetto di dispositivo a un personal computer o a uno *smartphone*. Eppure, attualmente esistono supercomputer che occupano ciascuno un intero capannone. Al contrario, esistono anche dispositivi i cui componenti sono sparsi in tutto il mondo.
- 10 Il dispositivo può funzionare in modo **isolato** o interconnesso. Prima della diffusione di Internet a metà degli anni '90, la maggior parte dei dispositivi funzionava in modo isolato. Da allora, questa modalità di funzionamento costituisce piuttosto l'eccezione, riservata a situazioni che richiedono un livello massimo di sicurezza, in particolare per evitare qualsiasi intrusione tramite connessioni esterne.
- 11 I dispositivi sono **interconnessi** quando sono collegati tra loro tramite una connessione cablata o wireless, come onde radio, collegamenti a infrarossi, fibra ottica o collegamenti satellitari, formando così una rete. Questa può essere limitata a una determinata area geografica, ad esempio un'abitazione, un'azienda o un'università. Si tratta in questo caso di una rete locale (*Local Area Network* o LAN). Tale rete può tuttavia estendersi anche su un'area molto più vasta, ad esempio una città, un paese o un continente. Si parla allora di rete estesa (*Wide Area Network* o WAN). La rete estesa più grande è Internet, poiché si tratta di una rete formata da una moltitudine di reti interconnesse che si estendono in tutto il mondo.
- 12 Infine, il concetto di dispositivo comprende anche gli **altri apparecchi** che consentono ai computer collegati alle reti di scambiarsi dati. A tal proposito, anche i server, i router, gli *switch*, i modem e i *gateway* devono essere considerati dispositivi.

B. Un programma

Agli elementi hardware si contrappongono gli elementi software, che 13
raggruppano l'insieme dei programmi che consentono **il funzionamento e l'utilizzo** dei diversi componenti del sistema informatico.

Un programma può essere definito come un **insieme di comandi** che, 14
quando vengono eseguiti da un sistema informatico, consentono di ottenere un risultato determinato.

Proprio come per i componenti hardware, è opportuno distinguere i 15
programmi in base al compito che svolgono. Il programma di «avvio» di qualsiasi sistema informatico è il **BIOS** (*Basic Input and Output System*) o l'**UEFI** (*Unified Extensible Firmware Interface*). È contenuto in un chip collegato alla scheda madre e fornisce gli elementi necessari all'avvio del sistema. Inoltre, garantisce la gestione di base dei diversi componenti hardware del sistema informatico e funge da interfaccia tra questi componenti e il sistema operativo.

Il **sistema operativo** costituisce, dal canto suo, il programma centrale del 16
sistema informatico. Assicura il funzionamento globale e coerente del sistema coordinando le diverse richieste inviate al sistema informatico dall'utente, nonché le interazioni tra i componenti hardware e gli altri programmi. In altre parole, il sistema operativo funge da interfaccia essenziale tra i software applicativi e gli elementi hardware del sistema.

Infine, i programmi applicativi svolgono ciascuno una **funzione** specifica. Ad 17
esempio, Word[®] consente l'elaborazione di testi, Photoshop[®] l'elaborazione di immagini, Outlook[®] la ricezione e l'invio di e-mail. Questi programmi si avvalgono tuttavia del sistema operativo per accedere alle risorse hardware ed eseguire le attività per cui sono stati progettati.

C. Il trattamento automatico dei dati

L'elaborazione automatizzata dei dati indica il fatto che i dati vengono 18
elaborati in modo automatico da un programma, **senza** che sia necessario un **intervento umano** diretto. Tale elaborazione può riguardare sia l'acquisizione che l'archiviazione o la restituzione dei dati.

Come si vedrà più avanti al punto III, i dati costituiscono informazioni digitali 19
immateriali. Per poter essere elaborati da un sistema informatico, le

informazioni provenienti dal mondo materiale devono essere convertite in un **linguaggio comprensibile dal dispositivo**. Pertanto, la pressione esercitata su un tasto della tastiera, su un pulsante del mouse o su un touchscreen viene tradotta in linguaggio binario e trasformata in segnali elettrici, logici o ottici.

- 20 Una volta che l'informazione materiale è stata convertita in segnali elettrici, logici o ottici, il programma è in grado di procedere all'elaborazione automatizzata dei dati. Una volta completata l'elaborazione, i dati vengono nuovamente tradotti in un **linguaggio comprensibile per l'utente**. Il programma può così, ad esempio, visualizzare caratteri alfabetici su uno schermo quando un utente preme i tasti di una tastiera, trasmettere le informazioni visive visualizzate sullo schermo a una stampante affinché vengano riprodotte su carta quando l'utente clicchi sull'icona «stampa» oppure stabilire una comunicazione telefonica quando l'utente preme il simbolo del telefono verde sul touchscreen del proprio *smartphone*. Ogni istruzione impartita dall'utente al sistema informatico genera la creazione di dati informatici, i quali vengono elaborati in modo automatizzato dai programmi e poi restituiti all'utente in una forma a lui comprensibile.

D. Prospettive

1. La dematerializzazione dei sistemi informatici

- 21 Già a partire dagli anni '80 è emersa l'idea dell'informatica distribuita, in particolare attraverso lo slogan lanciato da Sun Microsystems: «*The network is the computer!*» («La rete è il computer!»). Questo approccio si basa sulla **condivisione delle risorse** di calcolo al fine di elaborare volumi di dati più consistenti. In questa prospettiva, quando la rete in questione è Internet, il «computer» che essa rappresenta è costituito dall'insieme dei computer ad essa collegati, il che comporta una capacità di calcolo particolarmente considerevole. È in questo contesto che, a partire dalla fine degli anni '90 e con la diffusione di Internet, sono emersi progetti di calcolo distribuito. Questi progetti consistono nell'offrire ai privati la possibilità di mettere a disposizione, tramite Internet, la potenza di calcolo dei propri computer personali quando non li utilizzano, al fine di eseguire calcoli che richiedono capacità di elaborazione molto elevate.
- 22 Con il passare del tempo, questa logica di condivisione non si è più limitata al solo processore. È l'intera architettura informatica che è stata

progressivamente ripensata per diventare un'**architettura distribuita**, nel senso che le diverse risorse disponibili non si trovano più necessariamente nello stesso luogo né sulla stessa macchina. Un esempio emblematico di architettura distribuita che ha conosciuto un'ascesa fulminea all'inizio degli anni 2000 è il modello detto «peer-to-peer» (*peer-to-peer*). Questo modello consente la condivisione di file all'interno di un'architettura in cui ogni computer svolge contemporaneamente il ruolo sia di client che di server.

Tra la fine degli anni 2000 e l'inizio degli anni 2010 è apparso il *cloud computing* («informatica in nuvola»), che consiste nel ricorrere a server informatici remoti, connessi a Internet, per archiviare, gestire ed elaborare dati, anziché affidarsi a un server locale o a un computer personale. Questa tecnica consente in particolare all'utente di creare un sistema informatico virtuale, di installarvi un sistema operativo e delle applicazioni e di generare, elaborare e salvare dati al suo interno. A tal fine è sufficiente disporre di un terminale connesso a Internet, poiché tutte le altre risorse vengono messe a disposizione in modo virtuale e decentralizzato, provenienti da luoghi e talvolta da diversi fornitori di servizi sparsi in tutto il mondo. In una configurazione di questo tipo, risulta facile comprendere che la qualifica di «sistema» possa diventare problematica, dal momento che non esiste più un'unità fisica dei componenti.

2. L'Internet delle cose (IoT)

Da alcuni anni si assiste a una vera e propria esplosione del numero di **oggetti connessi**. Che si tratti di orologi, forni, televisori o veicoli, la quasi totalità degli oggetti di uso quotidiano esiste in una forma che può essere connessa a Internet.

Negli anni '90, SCHMID affermava, basandosi sul Messaggio del Consiglio federale, che i distributori automatici di cibo, benzina, biglietti, le fotocopiatrici o le slot machine non potessero essere qualificati come sistemi informatici, in quanto il legislatore federale aveva voluto limitare la nozione di sistema informatico ai soli dispositivi in grado di svolgere **le cosiddette «funzioni superiori»**.

Questa opinione non è più sostenibile oggi. Gli oggetti connessi fanno ormai pienamente parte di Internet, possono essere controllati a distanza e sono in grado di eseguire così tante attività da soddisfare tutti i criteri che consentono

di qualificarli come sistemi informatici ai sensi dell'art. 1 lett. a CCC. Questo **cambiamento di paradigma** solleva tuttavia seri problemi. Gli oggetti connessi, infatti, non beneficiano generalmente di misure di protezione equivalenti a quelle dei computer tradizionali. I criminali informatici possono quindi accedere più facilmente e indebitamente a un orologio connesso per estrarne i mezzi di pagamento che vi sono contenuti, sbloccare una porta collegata a un sistema domotico per introdursi in un'abitazione o ancora accedere a una rete aziendale collegandosi senza autorizzazione alla macchina da caffè connessa della propria mensa, rispetto all'accesso a un computer personale appositamente protetto contro qualsiasi accesso. Ne consegue che l'ambito di applicazione dell'art. 2 CCC, per gli Stati che non richiedono, come la Svizzera, che il reato sia commesso in violazione delle misure di sicurezza, risulta particolarmente ampio ed è destinato ad ampliarsi ulteriormente nei prossimi anni.

3. L'intelligenza artificiale

- 27 Come visto in precedenza (al punto II, lettera B), la definizione di cui all'art. 1 lett. a CCC presuppone che un sistema informatico sia dotato di un programma. Tale programma esegue in linea di principio una serie di comandi predefiniti dall'uomo. Con l'affermarsi dell'intelligenza artificiale, il **carattere immutabile dei programmi** non è più necessariamente scontato. I sistemi basati sull'intelligenza artificiale sono infatti in grado di apprendere in modo autonomo e possono, in determinate configurazioni, modificare il proprio codice sorgente o adattare i parametri dell'ambiente in cui operano. Si pone quindi la questione se il concetto di sistema informatico, così come è attualmente definito, rimanga sufficientemente ampio da comprendere tali evoluzioni tecnologiche o se sia necessaria una ridefinizione per tenere conto dei futuri sviluppi nel campo dell'intelligenza artificiale. A nostro avviso, la definizione attuale è formulata in modo sufficientemente ampio da includere le evoluzioni tecnologiche note fino ad oggi. Infatti, anche se l'intelligenza artificiale è in grado di riscrivere il codice sorgente di un programma per adattarsi al proprio ambiente, il sistema informatico continua a funzionare sulla base di un programma.
- 28 **Due problematiche** emergenti potrebbero tuttavia richiedere una ridefinizione nei prossimi anni. La prima riguarda l'intelligenza artificiale agentica autonoma e distribuita, ovvero agenti in grado di negoziare, migrare

tra ambienti, creare altri agenti o modificare la propria infrastruttura senza intervento umano. Ciò solleva il problema dell'unità del sistema informatico, poiché non si riuscirebbe più a determinare chiaramente a partire da quando uno sciame di agenti costituisca ancora un unico sistema informatico o più sistemi. Inoltre, la Convenzione non tiene conto del concetto di sistema informatico effimero, distribuito e auto-organizzato. La seconda problematica riguarda l'intelligenza artificiale neuromorfica, ovvero priva di programmi separati. Lo si vede, ad esempio, con i chip Loihi di Intel che imitano il cervello umano. A differenza dei processori tradizionali, questi chip elaborano le informazioni per eventi e integrano la memoria nel processore. Non esiste quindi più un «programma » distinto dall'hardware. L'esecuzione e l'apprendimento sono indissociabili, per cui l'attuale definizione di sistema informatico diventerebbe obsoleta.

A medio termine, sarebbe quindi necessario **estendere la definizione** di sistema informatico, da un lato, agli agenti autonomi dispiegati e, dall'altro, a qualsiasi dispositivo hardware o ibrido che effettui un'elaborazione dei dati tramite apprendimento, anche quando l'esecuzione non si basa su un programma distinto. 29

III. DATI INFORMATICI (LETT. B)

I dati informatici sono definiti come «*qualsiasi rappresentazione di fatti, informazioni o concetti in una forma che si presti al trattamento informatico, compreso un programma atto a far sì che un sistema informatico esegua una funzione*» (art. 1 lett. b CCC). Questa definizione, ripresa da quella dell'Organizzazione internazionale per la normazione (ISO), si caratterizza per la sua **neutralità tecnologica**. Ciò le conferisce il vantaggio di aver resistito in modo notevole alla fulminea evoluzione delle tecnologie dall'adozione della Convenzione nel 2001. 30

A. La forma dei dati

I sistemi informatici utilizzano un **linguaggio** fondamentalmente diverso da quello umano. Un testo, un'immagine o un'opera musicale realizzata dall'uomo non ha, di per sé, alcun significato per un computer. Per poter essere compresa ed elaborata, tale informazione deve essere convertita in un linguaggio comprensibile per la macchina. È in questa prospettiva che la definizione di «dati informatici» adottata nella Convenzione utilizza i termini 31

«che si prestano a un trattamento». Ciò significa che la rappresentazione di fatti, informazioni o concetti deve poter essere trattata direttamente da un sistema informatico, senza richiedere una trasformazione preliminare volta a consentirne il riconoscimento da parte di quest'ultimo. I dati informatici sono quindi informazioni che possono essere direttamente comprese e utilizzate da un computer.

- 32 L'informatica si basa su un **sistema binario**, il che significa che utilizza solo i numeri 0 e 1. Questa unità elementare di informazione è chiamata *bit*. Una sequenza di otto bit costituisce un byte (ad es. 10011101), che permette di rappresentare 2^8 , ovvero 256 valori distinti. Questo sistema rende possibile la traduzione delle informazioni provenienti dal linguaggio umano in indicazioni comprensibili dalla macchina. A seconda del programma utilizzato, un byte può rappresentare una cifra, una lettera, un colore o persino un suono. Ad esempio, quando un utente preme il tasto «a» sulla tastiera del proprio computer in un programma di elaborazione testi, questa azione viene convertita in linguaggio binario sotto forma di «01100001». Questo byte costituisce un dato che il computer è in grado di elaborare visualizzando una «a» sullo schermo. Allo stesso modo, i colori vengono convertiti in valori distribuiti su tre assi: rosso, verde e blu. Il valore 0 indica che il colore è assente, mentre il valore 255 indica che il colore ha la massima intensità. Pertanto, un pixel di colore albicocca in un programma di disegno sarà rappresentato dai valori 230 sulla scala del rosso, 126 sulla scala del verde e 48 sulla scala del blu, ovvero, in linguaggio binario, «11100110111111011000000». Questo dato a 24 bit permette al programma di disegno di visualizzare un pixel color albicocca sulla pagina bianca.
- 33 Gli esempi precedenti illustrano che, nell'informatica, il dato informatico è l'unità elementare che contiene un'informazione. Al contrario, quando un insieme di dati viene riunito per formare un tutto coerente, si parla di **file**. Può trattarsi di un testo, di un'immagine, di un video o di una registrazione audio.

B. I tipi di dati

- 34 La definizione dell'art. 1 lett. b CCC **non opera alcuna distinzione** tra i diversi tipi di dati. Sono interessati tutti i dati informatici, siano essi personali o meno, privati o pubblici, comprensibili dall'uomo o esclusivamente dalla macchina. Anche il contenuto dei dati è irrilevante, che si tratti di dati fattuali

(date, ore, misure, ecc.), di informazioni (rapporti, analisi, ecc.) o di concetti astratti (modelli, algoritmi, codici, ecc.). Costituiscono quindi dati ai sensi dell'art. 1 lett. b CCC i dati memorizzati su supporti di archiviazione, i dati temporanei, i dati in transito, i metadati e persino i dati crittografati.

Ai dati creati dall'uomo occorre, a nostro avviso, aggiungere quelli prodotti automaticamente da un sistema informatico a partire da dati preesistenti, denominati **dati derivati o inferiti**, in particolare mediante processi di trasformazione, di combinazione o di analisi algoritmica. A titolo di esempio, si possono citare i profili degli utenti, i punteggi, le previsioni o le classificazioni generate senza un intervento umano diretto. Sebbene non si tratti di dati inizialmente forniti da un utente, a nostro avviso devono essere inclusi nella definizione di cui all'art. 1 lett. b CCC, purché si prestino a un trattamento informatico e siano utilizzabili da un sistema informatico. 35

La definizione di dati informatici si estende, a nostro avviso, anche ai dati **volatili** (o effimeri), in particolare quelli memorizzati temporaneamente nella memoria RAM di un sistema, generati dinamicamente durante l'esecuzione di un programma o destinati a scomparire automaticamente dopo un lasso di tempo molto breve. Sebbene la loro durata sia breve, rivestono particolare importanza nell'ambito delle indagini penali, in particolare in caso di accesso illegale (art. 2 CCC) o di violazione dell'integrità del sistema (art. 5 CCC) mediante un attacco di tipo «denial of service distribuito». 36

Alla luce della definizione di dati informatici incentrata esclusivamente sulla funzione, è irrilevante che i dati siano comprensibili per un essere umano. I dati rimangono dati informatici anche quando sono **crittografati, compressi, frammentati** o archiviati in una forma che non ne consente la lettura immediata. La crittografia dei dati non è rilevante dal punto di vista giuridico, poiché costituisce solo una modalità tecnica di trattamento dei dati volta a limitarne l'accesso. Di conseguenza, lo status giuridico dei dati non cambia per il fatto che essi siano crittografati o resi temporaneamente inutilizzabili dai criminali informatici. 37

C. I programmi

La precisazione «compreso un programma», voluta dai redattori della Convenzione, mira a eliminare ogni ambiguità riguardo all'inclusione dei **programmi** nella definizione di cui all'art. 1 lett. b CCC. Questo approccio è 38

del tutto coerente sotto due aspetti. Dal punto di vista informatico, un programma è un insieme di istruzioni contenute in un codice sorgente, a sua volta composto da una moltitudine di caratteri, ovvero dati, che determinano il modo in cui i dati che gli vengono forniti devono essere trattati. Da un punto di vista sistematico, l'inclusione dei programmi nella definizione di dati informatici rientra nella volontà chiaramente affermata dai redattori della Convenzione di non operare alcuna distinzione tra i diversi tipi di dati.

D. Prospettive

- 39 Sebbene al momento della redazione della Convenzione fosse impossibile prevedere i futuri sviluppi dell'informatica, la scelta di una definizione **tecnologicamente neutra** ha permesso di includervi tutti i nuovi tipi di dati emersi dal 2001. È il caso, in particolare, delle criptovalute, dei dati generati dagli oggetti connessi e dei *dataset*, ovvero le raccolte strutturate di dati destinate all'addestramento di modelli di apprendimento automatico.

E. Excursus: la distinzione tra dati relativi all'abbonato, dati relativi al traffico e dati di contenuto nel diritto penale svizzero

- 40 La rapida evoluzione delle tecnologie negli ultimi trent'anni ha reso necessari **adeguamenti legislativi di grande rilevanza** al fine di distinguere quali tipi di dati potessero essere ottenuti e a quali condizioni. La prima Legge sulla sorveglianza della corrispondenza postale e delle telecomunicazioni (LSCPT) è stata adottata il 6 ottobre 2000 ed è entrata in vigore il 1^{er} gennaio 2002. È stata completamente rivista nel 2016, per poi subire diverse revisioni parziali, tra cui una particolarmente significativa nel 2024.
- 41 Il legislatore ha ritenuto che non tutti i dati avessero la stessa importanza. È partito dal presupposto che quanto più grave fosse la violazione della sfera privata, garantita dall'art. 13 Cost., tanto più rigorose dovessero essere le condizioni alle quali tali dati potevano essere ottenuti. La legge opera quindi una distinzione tra **tre tipi di dati**: i dati relativi all'abbonato (*Bestandesdaten*), i dati relativi al traffico (*Randdaten*) e i dati di contenuto (*Inhaltsdaten*).
- 42 La Convenzione sulla criminalità informatica opera la stessa distinzione al suo articolo 18.

1. I dati relativi all'abbonato

I dati relativi all'abbonato comprendono le **informazioni di identificazione del titolare** di un allacciamento. Si tratta in particolare del cognome, del nome, della data di nascita, dell'indirizzo e, se nota, della professione dell'utente (art. 21 cpv. 1 lett. a LSCPT), nonché delle risorse di indirizzamento (art. 21 cpv. 1 lett. b LSCPT) e dei tipi di servizi (art. 21 cpv. 1 lett. c LSCPT) che sono stati utilizzati. 43

Tali dati corrispondono a quelli elencati all'**art. 18 cpv. 3 CCC**, ovvero: il tipo di servizio di comunicazione utilizzato, le disposizioni tecniche adottate a tal fine e il periodo di servizio (lett. a); l'identità, l'indirizzo postale o geografico e il numero di telefono dell'abbonato, nonché qualsiasi altro numero di accesso, i dati relativi alla fatturazione e al pagamento, disponibili sulla base di un contratto o di un accordo di servizi (lett. b); qualsiasi altra informazione relativa all'ubicazione delle apparecchiature di comunicazione, disponibile sulla base di un contratto o di un accordo di servizi (lett. c) . 44

Si tratta dei **dati meno sensibili**. Il loro ottenimento comporta solo una minima violazione della sfera privata. Nel diritto svizzero, il loro ottenimento è quindi soggetto esclusivamente alle condizioni di cui all'art. 197 cpv. 1 CPP e non richiede l'autorizzazione del Tribunale delle misure coercitive. 45

2. I dati relativi al traffico (o dati secondari)

I dati relativi al traffico sono i dati che indicano con **chi, quando, per quanto tempo e da dove** la persona sorvegliata è stata o è in comunicazione, nonché le caratteristiche tecniche della comunicazione in questione (art. 8 lett. b LSCPT). 46

In una sentenza di principio, il Tribunale federale ha in particolare ritenuto che **la cronologia degli indirizzi IP** degli utenti che si sono collegati a un social network rientri nei dati relativi al traffico e non in quelli relativi all'abbonato. Questa sentenza, che è stata oggetto di aspre critiche in dottrina, è stata recentemente confermata in una sentenza non pubblicata. 47

La Convenzione sulla criminalità informatica li definisce all'art. 1 lett. d CCC. Essi saranno esaminati in dettaglio nel capitolo V che segue. 48

Questi **dati** sono **più sensibili** rispetto ai dati relativi all'abbonato. Il legislatore svizzero ha quindi deciso di imporre requisiti più rigorosi per il 49

loro ottenimento. È quindi necessario che siano soddisfatte cumulativamente le condizioni di cui all'art. 197 cpv. 1 e 273 cpv. 1 CPP. L'ottenimento di tali dati è quindi possibile solo in presenza di gravi sospetti che facciano presumere che sia stato commesso un crimine o un delitto. Semplici supposizioni o vaghi sospetti non sono sufficienti. L'ottenimento di tali dati non è possibile nemmeno in caso di contravvenzione. A ciò si aggiunge che l'ottenimento deve essere giustificato alla luce della gravità del reato (principio di proporzionalità) e che le misure adottate fino a quel momento nell'ambito dell'istruttoria siano rimaste senza esito oppure che le indagini non avrebbero alcuna possibilità di successo o sarebbero eccessivamente difficili in assenza di sorveglianza (principio di sussidiarietà).

- 50 L'acquisizione di tali dati è inoltre possibile solo con l'**autorizzazione** del Tribunale delle misure coercitive (art. 274 CPP).

3. I dati di contenuto

- 51 I dati di contenuto corrispondono alla **sostanza** stessa **delle comunicazioni** (art. 8 lett. a LSCPT). Si tratta dell'espressione scritta o orale del pensiero umano, in particolare del testo redatto dall'autore di un'e-mail o di un messaggio oppure delle parole pronunciate da un interlocutore durante una conversazione telefonica.
- 52 La sorveglianza dei dati di contenuto è **la forma di sorveglianza più invasiva** e costituisce la violazione più grave del segreto delle telecomunicazioni e della sfera privata. È quindi ovvio che i requisiti stabiliti dal legislatore svizzero siano i più elevati tra i tre tipi di dati.
- 53 I dati di contenuto sono menzionati all'art. 21 CCC. Anche i redattori della Convenzione ritenevano che tali dati non potessero essere ottenuti per perseguire qualsiasi reato. Hanno quindi integrato il **principio di proporzionalità**, prevedendo che tali dati potessero essere raccolti solo per perseguire determinati reati gravi che dovevano essere definiti nel diritto interno.
- 54 La raccolta dei dati di contenuto è disciplinata dall'**art. 269 CPP**. Essa richiede l'esistenza di gravi sospetti che facciano presumere la commissione di un crimine o di un delitto elencati in modo esaustivo all'art. 269, comma 2, del CPP. Anche in questo caso, semplici supposizioni o vaghi sospetti non sono sufficienti. L'acquisizione di tali dati deve inoltre essere giustificata alla

luce della gravità del reato (principio di proporzionalità). Non è quindi sufficiente che il reato perseguito figuri nell'elenco di cui all'art. 269 cpv. 2 CPP, ma occorre inoltre che la gravità concreta del reato nel caso di specie giustifichi la misura di sorveglianza. Infine, le misure adottate fino a quel momento nell'ambito dell'istruttoria devono essersi rivelate infruttuose oppure le indagini non avrebbero alcuna possibilità di esito positivo o risulterebbero eccessivamente difficili in assenza di sorveglianza (principio di sussidiarietà).

Proprio come per i dati relativi al traffico, l'acquisizione dei dati di contenuto 55 è possibile solo con l'**autorizzazione** del Tribunale delle misure coercitive (art. 274 CPP).

IV. FORNITORE DI SERVIZI (LETT. C)

Ai sensi dell'art. 1 lett. c CCC, « *per « fornitore di servizi » si intende qualsiasi 56 ente pubblico o privato che offra agli utenti dei propri servizi la possibilità di comunicare tramite un sistema informatico, nonché qualsiasi altro ente che tratti o conservi dati informatici per tale servizio di comunicazione o per i suoi utenti* ». Questa definizione opera una distinzione tra **due tipi** di fornitori: i fornitori di accesso e i fornitori di archiviazione o di contenuti.

A. I fornitori di accesso

I fornitori di servizi di cui all'art. 1 lett. c n. 1 CCC sono i fornitori di accesso 57 (*access provider*), ovvero coloro che consentono agli utenti di **connettersi a una rete** e di **comunicare tra loro** tramite un sistema informatico.

Si tratta in primo luogo degli operatori di telecomunicazioni (ad es. Swisscom, 58 SFR, Deutsche Telekom, Vodafone, TIM) che consentono ai privati di connettersi a Internet. A nostro avviso, questa definizione deve essere intesa in senso molto più ampio ed estendersi a tutte le **entità che forniscono l'accesso a una rete** tramite un sistema informatico. Sono quindi interessate le imprese private o gli enti pubblici che mettono a disposizione degli utenti punti di accesso a Internet (ad es. le compagnie ferroviarie, gli alberghi, i comuni, ecc.), le imprese private o gli enti pubblici che gestiscono una rete privata e forniscono ai propri utenti l'accesso a tale rete, nonché i privati che dispongono di un punto di accesso a Internet o a una rete domestica, in

particolare sotto forma di hotspot Wi-Fi, e che offrono a terzi la possibilità di connettersi ad essa.

- 59 Questa **interpretazione estensiva** è confermata dai redattori della Convenzione, i quali sottolineano nella loro Relazione esplicativa che è irrilevante che gli utenti costituiscano un gruppo chiuso o che il fornitore offra o meno i propri servizi al pubblico, gratuitamente o a pagamento. Il gruppo chiuso può essere costituito dai dipendenti di un'impresa privata ai quali i servizi sono forniti tramite una rete aziendale.
- 60 A nostro avviso, la formulazione «che offre agli utenti dei propri servizi la possibilità di comunicare» comprende non solo gli enti pubblici o privati che forniscono l'accesso alla rete, ma anche tutti coloro che **rendono materialmente possibile la comunicazione**. Il concetto di «fornitore di accesso» si estende quindi a tutti i soggetti che mettono a disposizione un'infrastruttura o un servizio che consenta la trasmissione, l'instradamento o l'inoltro dei dati attraverso la rete, purché offrano agli utenti un servizio funzionale di comunicazione. Non rientrano invece in tale ambito gli attori puramente tecnici o industriali, che si limitano alla fabbricazione, alla fornitura o alla manutenzione di apparecchiature senza offrire essi stessi un servizio di comunicazione.
- 61 Da un punto di vista puramente funzionale, la definizione di cui all'art. 1 lett. c n. 1 CCC riguarda anche alcune categorie di **soggetti intermedi della rete** che, pur non fornendo un accesso classico a Internet, svolgono un ruolo determinante nell'effettiva possibilità di comunicare tramite un sistema informatico. È il caso, in particolare, dei fornitori di servizi di reti private virtuali (*Virtual Private Network* o VPN), che garantiscono ai propri utenti un accesso sicuro e anonimo alle risorse accessibili tramite la rete, combinando funzioni di instradamento, trasmissione e crittografia delle comunicazioni.
- 62 Sempre dal punto di vista funzionale, possono rientrare nell'ambito di applicazione dell'art. 1 lett. c n. 1 CCC anche gli **operatori di servizi di infrastruttura** essenziali per la comunicazione su Internet, quali i fornitori di servizi di risoluzione dei nomi di dominio (DNS) accessibili al pubblico o gli operatori di punti di scambio Internet (*Internet Exchange Points* o IXP), purché offrano un servizio che consenta l'instradamento o l'interconnessione delle comunicazioni tra utenti o fornitori di reti.

B. I fornitori di spazio di archiviazione o di contenuti

I **fornitori di servizi** di cui all'art. 1 lett. c n. 2 CCC sono coloro che mettono a disposizione, a titolo gratuito o a pagamento, spazi di archiviazione (*hosting providers*) o contenuti per i siti web (*content providers*). 63

I **fornitori di spazio di archiviazione** (*hosting provider*) sono soggetti che offrono agli utenti di Internet server che consentono l'archiviazione o il trattamento dei dati. Si suddividono in **due categorie**: quelli che archiviano o trattano dati per conto dei soggetti di cui al punto (i) e quelli che archiviano o trattano dati per conto degli utenti dei servizi offerti dai soggetti di cui al punto (ii): 64

La prima categoria comprende i fornitori di servizi di archiviazione che trattano o conservano i dati dei **fornitori di accesso**. Si tratta in particolare dei dati relativi al traffico (cfr. punto V di seguito), dei dati del sistema dei nomi di dominio (*Domain Name System* o DNS) che associa i nomi di dominio all'indirizzo IP dei server su cui sono ospitati, nonché dei dati relativi ai diversi server attraverso i quali transitano le e-mail. 65

La seconda categoria riguarda i fornitori che archiviano o trattano i dati degli **utenti** dei fornitori di accesso. Sono interessati, in particolare, i soggetti che ospitano siti web, che offrono spazi per l'implementazione di sistemi informatici virtuali, o ancora ambienti in cui i dati possono essere salvati, gestiti o trattati a distanza (*cloud computing*). 66

Nel contesto del *cloud computing*, la qualifica di fornitore di servizi ai sensi dell'art. 1 lett. c n. 2 CCC si applica indifferentemente ai diversi modelli di servizi comunemente distinti, vale a dire l'infrastruttura come servizio (*Infrastructure as a Service* o IaaS), la piattaforma come servizio (*Platform as a Service* o PaaS) e il software come servizio (*Software as a Service* o SaaS). Indipendentemente dalla forma scelta, questi modelli comportano tutti l'archiviazione, l'elaborazione o la messa a disposizione di dati informatici per conto di terzi, il che ne giustifica l'inclusione nella definizione di fornitori di servizi di cui all'art. 1 lett. c n. 2 CCC. 67

Rientrano inoltre tra i fornitori di servizi i soggetti che gestiscono **reti di distribuzione di contenuti** 68

(*Content Delivery Networks* o CDN). Questi soggetti garantiscono la memorizzazione nella cache, l'archiviazione temporanea e la distribuzione ottimizzata dei dati tramite server distribuiti geograficamente.

- 69 La definizione di cui all'art. 1 lett. c n. 2 CCC non è tuttavia destinata ad applicarsi a un semplice fornitore di contenuti (ad es. a una persona che stipula un contratto con un fornitore di hosting affinché questo ospiti il suo sito web), qualora quest'ultimo non offra inoltre servizi di comunicazione o altri servizi di trattamento dei dati. Al contrario, rientrano a nostro avviso nell'ambito di applicazione della definizione di cui all'art. 1 lett. c n. 2 CCC i siti web che, oltre alla messa a disposizione di contenuti, forniscono **servizi di comunicazione**, quali i siti web che mettono a disposizione caselle di posta elettronica, servizi di messaggistica istantanea o forum di discussione. Lo stesso vale per i siti web che offrono **servizi di trattamento dei dati**, in particolare la crittografia dei dati, la traduzione di testi, l'analisi finanziaria dei dati o ancora la raccolta automatizzata di dati non strutturati e la loro conversione in dati organizzati (*web scraping*).
- 70 Questa analisi si applica anche alle **piattaforme online** e ai **social network** che, oltre alla diffusione di contenuti, offrono funzionalità strutturate di comunicazione e interazione tra gli utenti. Tali servizi comportano generalmente la creazione di account, lo scambio di messaggi, la pubblicazione di contenuti, nonché il trattamento automatizzato dei dati a fini di classificazione, pubblicità mirata o moderazione.

C. Prospettive

- 71 Infine, analogamente alla definizione adottata per i dati informatici, la definizione di fornitore di servizi è concepita in modo tecnologicamente neutro. Questo approccio ha permesso di integrare i **nuovi tipi di servizi** emersi dal 2001, in particolare i soggetti che offrono servizi basati sull'intelligenza artificiale per elaborare o generare dati. È tuttavia opportuno precisare che non è l'intelligenza artificiale in quanto tale ad essere oggetto della definizione, bensì le funzioni di archiviazione, trattamento o comunicazione dei dati informatici che essa consente di garantire.

V. DATI RELATIVI AL TRAFFICO (LETT. D)

L'ultima definizione fornita dalla convenzione figura all'art. 1 lett. d CCC, 72 secondo cui i dati relativi al traffico « *indicano tutti i dati relativi a una comunicazione che transita attraverso un sistema informatico, prodotti da quest'ultimo come elemento della catena di comunicazione, che indicano l'origine, la destinazione, l'itinerario, l'ora, la data, la dimensione e la durata della comunicazione o il tipo di servizio sottostante*». Questi dati rivestono uno **status giuridico particolare**, nella misura in cui possono fungere da indizi, o addirittura da prove, nelle indagini penali. Essi sono generati dai diversi sistemi informatici che intervengono nella catena di comunicazione al fine di instradare quest'ultima dal punto di origine alla destinazione. Costituiscono quindi elementi ausiliari della comunicazione stessa stessa.

I dati relativi al traffico sono necessari per individuare la **fonte della 73 comunicazione**; costituiscono un punto di partenza che consente di raccogliere ulteriori prove o un elemento costitutivo della prova del reato. Tuttavia, a causa del notevole volume di comunicazioni scambiate quotidianamente, i dati relativi a tali comunicazioni hanno una durata di conservazione molto limitata. È quindi essenziale agire con rapidità per ricostruire il percorso della comunicazione sospetta prima che le tracce scompaiano. Tenuto conto della durata spesso significativa delle procedure ordinarie di assistenza giudiziaria internazionale in materia penale, la Convenzione prevede la possibilità di ricorrere alla procedura di divulgazione rapida di cui all'art. 17 CCC. Questa consente di ottenere senza indugio informazioni sul percorso della comunicazione e di raccogliere altre prove prima che vengano cancellate, oppure di identificare un indagato. Questa procedura accelerata e meno formale rimane compatibile con il principio di proporzionalità, nella misura in cui l'ottenimento di dati relativi al traffico comporta una violazione sensibilmente minore dei diritti della personalità rispetto all'ottenimento di dati relativi al contenuto, poiché non rivela il contenuto della comunicazione, ma solo il suo percorso.

L'art. 1 lett. d CCC elenca in modo **esauriente** le categorie di dati relativi al 74 traffico soggette a un regime particolare nella Convenzione, ovvero: l'origine, la destinazione, l'itinerario, l'ora, la data, la dimensione e la durata della comunicazione o il tipo di servizio sottostante.

- 75 L'**origine** e la **destinazione** corrispondono ai punti della rete da cui una comunicazione viene emessa e ricevuta. Essi sono identificati, a seconda della modalità di comunicazione utilizzata, da numeri di telefono o, più in generale, da indirizzi IP assegnati ai sistemi informatici interessati in un determinato momento. Tali identificativi non consentono necessariamente di identificare direttamente un utente finale, in particolare in presenza di indirizzi IP dinamici, condivisi o occultati da procedure quali la traduzione degli indirizzi di rete (NAT), i servizi di relay (ad es. la rete TOR) o le reti private virtuali (VPN). Essi rivestono particolare importanza per le indagini penali, poiché consentono di individuare il sistema informatico o il punto di accesso alla rete all'origine o alla destinazione della comunicazione.
- 76 L'**itinerario** descrive il percorso seguito dalla comunicazione attraverso i diversi punti di transito della rete, in particolare router, server intermedi o altre infrastrutture di transito. Corrisponde alla successione dei sistemi informatici attraverso i quali i dati vengono instradati dal loro punto di origine alla loro destinazione. In pratica, tale percorso può essere ricostruito parzialmente o totalmente a partire dai dati generati da questi diversi sistemi, fatte salve le limitazioni tecniche legate in particolare all'architettura della rete, all'utilizzo di servizi intermedi o alla crittografia delle comunicazioni.
- 77 L'**ora** e la **data** sono espresse in tempo universale coordinato (UTC). Queste informazioni sono essenziali in presenza di indirizzi IP dinamici. Poiché tali indirizzi vengono riassegnati continuamente in base alle esigenze degli utenti, è indispensabile disporre di queste informazioni per poter chiedere al fornitore di accesso a quale sistema informatico abbia assegnato un indirizzo IP in un determinato momento. Tali informazioni devono essere ottenute nel più breve tempo possibile, poiché, a seconda degli Stati, vengono conservate solo per un periodo compreso tra sei e ventiquattro mesi al massimo. Una volta trascorso tale termine, i dati vengono distrutti e diventa impossibile identificare l'utente a cui è stato assegnato un indirizzo IP. Tale difficoltà non sussiste invece con gli indirizzi IP statici, poiché questi sono assegnati in modo permanente agli stessi utenti.
- 78 La **dimensione** della comunicazione è espressa in bit o in byte e corrisponde al volume di dati scambiati. Può costituire un indizio per gli investigatori sul tipo di dati scambiati, nella misura in cui alcuni tipi di contenuti, quali immagini, registrazioni sonore o contenuti audiovisivi, generano in linea di principio volumi di dati più consistenti rispetto ai semplici messaggi di testo.

Tale indicatore deve tuttavia essere interpretato con cautela, tenendo conto delle attuali tecniche di compressione, frammentazione e crittografia dei flussi di dati.

La **durata** della comunicazione è misurata in ore, minuti e secondi. 79
Corrisponde al lasso di tempo durante il quale è stata stabilita una comunicazione o ha avuto luogo uno scambio di dati tra i sistemi informatici interessati. Questa informazione può fornire elementi contestuali utili alle indagini, in particolare per distinguere le comunicazioni sporadiche dalle connessioni prolungate o ripetute, senza tuttavia rivelare il contenuto degli scambi avvenuti durante tale periodo.

Infine, il **tipo di servizio sottostante** si riferisce alla modalità di 80
comunicazione o alla categoria funzionale del servizio utilizzato nell'ambito dello scambio di dati, quali la posta elettronica, i servizi di messaggistica istantanea, la visualizzazione di contenuti audiovisivi online o il download di dati. Si tratta di una qualificazione generale del servizio utilizzato, che può risultare difficile da stabilire con precisione quando più servizi sono combinati all'interno dello stesso flusso di comunicazione o quando i dati sono incapsulati o crittografati.

BIBLIOGRAFIA

Schmid Niklaus, Computer- sowie Check- und Kreditkartenkriminalität, Zurich 1994.

I MATERIALI

Conseil de l'Europe, Explanatory Report to the Convention on Cybercrime, Budapest 23.11.2001, disponible sous <https://rm.coe.int/16800cce5b>, visité le 10.01.2026 (cité : Rapport explicatif de la Convention sur la cibercriminalité).

Comité de la Convention cibercriminalité (T-CY), Guidance Notes, disponible sous <https://www.coe.int/fr/web/cybercrime/guidance-notes>, visité le 10.01.2026 (cité : Note d'orientation).

ATTENZIONE: Questa versione del commentario è una traduzione automatica dell'originale. Il commentario originale è in francese. La traduzione è stata effettuata con www.deepl.com. Solo la versione originale fa fede. La forma tradotta del commentario non può essere citata

COMMENTO SU

Art. 2 CCC (Convenzione sulla cibercriminalità [Cybercrime Convention])

Un commentario di Jérémie Müller

CITAZIONE SUGGERITA

Jérémie Müller, Commentario all'art. 2 CCC, in: Damian K. Graf (a cura di), Commentario online alla Convenzione sulla cibercriminalità [Cybercrime Convention]

Breve citazione: OK-Müller, art. 2 CCC N. XXX.

Capitolo II: Provvedimenti da adottare a livello nazionale

Sezione 1: Diritto penale materiale

Titolo 1: Reati contro la riservatezza, l'integrità e la disponibilità di dati e sistemi informatici

Art. 2 Accesso illecito

Le Parti adottano le misure legislative e di altra natura necessarie per definire come reato, nel loro diritto interno, l'accesso intenzionale e illecito a un sistema informatico o a parte di esso. Le Parti possono

prevedere che il reato debba essere commesso violando misure di sicurezza, con l'intenzione di reperire dati informatici, con altro intento illegale oppure in relazione a un sistema informatico collegato a un altro sistema informatico.

STRUTTURA

I. Generalità.....	32
II. Beni giuridicamente protetti	32
III. Elementi costitutivi fondamentali.....	33
A. Un sistema informatico	33
B. Accesso al sistema informatico	33
C. Illegalità	35
D. Intenzione	37
IV. Elementi costitutivi aggiuntivi facoltativi	37
A. Accesso in violazione delle misure di sicurezza.....	37
B. Lo scopo di ottenere dati informatici o un altro scopo specialeB. Lo scopo di ottenere dati informatici o un altro scopo speciale	38
C. Un sistema informatico collegato a un altro sistema informatico	39
V. Confronto con il diritto svizzero	40
Bibliografia	41
I Materiali	42

I. GENERALITÀ

- 1 L'accesso illegale a un sistema informatico è il reato base della criminalità informatica. Spesso è il presupposto necessario per la commissione di un altro reato informatico, come l'interferenza di dati (art. 4 CCC), l'interferenza di sistema (art. 5 CCC), la falsificazione informatica (art. 7 CCC) o la frode informatica (art. 8 CCC). Tuttavia, alcuni criminali informatici si accontentano di ottenere un accesso non autorizzato a un sistema informatico, per spavalderia o semplicemente per la sfida tecnica che rappresenta, senza commettere alcun reato successivo. È quindi giustificato incriminare questa condotta a sé stante, anziché farla confluire nei reati punibili ai sensi delle sezioni successive. Pertanto, l'autore del reato è colpevole di accesso illecito per il solo fatto di accedere a un sistema informatico. Non è necessario che rubi o modifichi i dati presenti nel sistema informatico.
- 2 Alcuni potrebbero considerare l'hacking come un'attività relativamente innocua e ludica, praticata da alcuni smanettoni in cerca di nuove sfide. Ma la realtà è ben diversa. Questo comportamento è molto più diffuso di quanto si possa pensare a prima vista e i suoi autori perseguono obiettivi molto meno onorevoli del semplice divertimento.
- 3 Naturalmente, il modo più efficace per proteggere un sistema informatico da accessi non autorizzati è rappresentato da solide misure di sicurezza. Data la minaccia che l'hacking rappresenta per la sicurezza dei sistemi informatici e dei dati, le misure tecniche devono essere accompagnate da misure legislative volte a dissuadere i criminali informatici dall'agire o a punirli se commettono atti dolosi. In questo modo, si tutelano al meglio gli interessi delle organizzazioni e dei singoli cittadini a poter gestire, operare e controllare i propri sistemi informatici senza interruzioni o impedimenti di alcun tipo.

II. BENI GIURIDICAMENTE PROTETTI

- 4 L'articolo 2 del Codice penale protegge l'inviolabilità dei sistemi informatici. Questa protezione penale è necessaria per almeno due motivi.
- 5 Da un lato, l'accesso illegale a un sistema informatico può comportare notevoli costi di riparazione per il legittimo proprietario. Gli autori dei reati spesso modificano i dati per poter accedere al sistema. Inoltre, le vittime

spesso si accorgono dell'intrusione solo qualche tempo dopo che è avvenuta. È quindi particolarmente difficile rintracciare ciò che è stato modificato dagli autori, nonché i nuovi dati generati dal sistema informatico in seguito a tale modifica. Una volta identificati, questi dati devono essere ripristinati allo stato originale. Queste operazioni possono essere molto lunghe e costose.

D'altro canto, l'accesso illegale consente agli autori di consultare informazioni a cui non dovrebbero avere accesso (ad esempio rapporti riservati, segreti commerciali, elenchi di clienti, documenti contabili, numeri di carte di credito, dati personali, ecc.) Queste informazioni possono poi essere rivendute sul mercato nero, con danni ancora maggiori per il titolare del diritto rispetto al semplice ripristino della protezione del sistema. 6

III. ELEMENTI COSTITUTIVI FONDAMENTALI

A. Un sistema informatico

Ai sensi dell'art. 1 let. a CCC, "per sistema informatico si intende qualsiasi dispositivo isolato o insieme di dispositivi interconnessi o collegati, che esegue o uno o più dei cui elementi esegue, in esecuzione di un programma, l'elaborazione automatica di dati". Il concetto di sistema informatico comprende quindi tutti gli elementi hardware (scheda madre, processore, disco rigido, schermo, tastiera, stampante, ecc.) e software (BIOS, sistema operativo, software, aggiornamenti, ecc.), nonché i dispositivi che consentono di collegare tra loro questi vari elementi (cavi, router, terminale wifi, ecc.). 7

Per maggiori dettagli su questo concetto, si rimanda a quanto scritto nel precedente art. 1 CCC. 8

B. Accesso al sistema informatico

Si potrebbe essere tentati di paragonare l'accesso illecito a un sistema informatico al reato di violazione di domicilio. L'accesso al sistema informatico sarebbe quindi l'equivalente digitale della violazione di domicilio. L'aspetto rassicurante di questa analogia è che è facile visualizzare la situazione a livello intellettuale. Tuttavia, il mondo virtuale è più complesso e i contorni dei concetti giuridici sono necessariamente più sfumati. 9

È complicato tracciare un'analogia con il mondo reale. Tuttavia, se si dovesse fare un'analogia, l'accesso a un sistema informatico potrebbe essere 10

paragonato all'ingresso in una fortezza medievale. L'accesso al castello è limitato da un muro di cinta e da un fossato. Il cancello d'ingresso principale è solitamente sorvegliato da guardie. Esse controllano che le persone che entrano nella fortezza siano autorizzate a farlo. Una volta entrati, gli individui possono accedere ad alcune parti del castello e non ad altre, a seconda del loro rango. Il rango è definito dal signore a cui appartiene il castello. Ogni parte del castello contiene oggetti che possono essere visti, toccati, modificati o addirittura distrutti. Anche per questi oggetti, il signore del castello stabilisce chi può fare cosa con quale oggetto. Il signore del castello è l'unica persona che ha accesso a tutte le stanze del castello e l'unica che può agire come meglio crede con tutti gli oggetti del castello.

- 11 Un sistema informatico funziona in modo simile a un castello. Per accedere al sistema informatico, l'utente deve generalmente inserire un nome utente e una password. Una volta effettuato l'accesso, gli utenti possono accedere a tutto o a parte del sistema informatico, a seconda del loro livello di accreditamento, che viene determinato dall'amministratore del sistema informatico. Questo livello di accreditamento determina anche ciò che l'utente può o non può fare nelle parti del sistema informatico a cui ha accesso, ad esempio visualizzare solo il titolo dei documenti contenuti in una cartella, aprirli per leggerli, modificarli o cancellarli. L'amministratore è l'unica persona che può accedere all'intero sistema informatico e ha il diritto di eseguire qualsiasi azione desideri con i dati in esso contenuti.
- 12 Tuttavia, l'analogia con il mondo reale finisce qui. Il concetto di "accesso" nel mondo virtuale non può essere paragonato a quello di "penetrazione" nel mondo reale. In informatica, la nozione di "accesso" significa che l'autore riesce a stabilire una connessione con tutto o parte di un sistema informatico. A rigore, quindi, non vi è alcuno spostamento fisico dell'autore da un luogo all'altro.
- 13 Nella forma semplice del reato, il mezzo utilizzato dall'autore per collegarsi al sistema informatico è irrilevante. L'autore può quindi stabilire una connessione mediante accesso locale o remoto. Se l'autore stabilisce una connessione locale con un sistema informatico a cui ha accesso fisico, lo farà utilizzando una tastiera - hardware o virtuale - e un mouse, o anche semplicemente con le dita nel caso di tablet e smartphone. Può anche utilizzare un terminale per collegarsi a un sistema informatico centrale. Se invece l'autore decide di stabilire una connessione remota, può utilizzare

qualsiasi rete di telecomunicazioni. Il tipo di rete (locale, pubblica, privata, ecc.) e il tipo di connessione (via cavo o wireless) sono irrilevanti.

Anche l'entità dell'accesso non è determinante ai fini della commissione del reato. L'accesso può essere totale, nel qual caso si estende all'intero sistema informatico. Può anche essere solo parziale. In questo caso, riguarda solo una parte del sistema informatico. È il caso, ad esempio, di chi accede solo alla sessione di un utente o a una parte dei dati memorizzati su un server. 14

Il reato viene commesso nel momento in cui viene stabilita la connessione al sistema informatico. Nulla impedisce quindi all'autore del reato di venire a conoscenza dei dati informatici contenuti nel sistema informatico. Tuttavia, non è necessario che l'autore del reato venga a conoscenza dei dati perché il reato sia stato commesso. Nella pratica, tuttavia, questi due eventi di solito coincidono, poiché i dati vengono visualizzati sullo schermo quando viene stabilito l'accesso. 15

Il concetto di accesso ai sensi dell'articolo 2 del Codice penale deve essere chiaramente distinto dall'interferenza dei dati ai sensi dell'articolo 4 del Codice penale. Per commettere il reato, è sufficiente che l'autore ottenga l'accesso a un sistema informatico. Anche se, in pratica, la creazione di un accesso illegale porta regolarmente alla modifica dei dati, tale deterioramento non è necessario per la commissione del reato. 16

Infine, solo la creazione di un accesso illegale è punibile. Il mantenimento di un accesso lecito dopo che il proprietario del sistema informatico ha informato l'utente che non è più autorizzato ad accedervi non è punibile. Un esempio è rappresentato da un dipendente che, nel corso del suo lavoro, utilizza il proprio computer privato per collegarsi alla rete aziendale e che, una volta licenziato, continua a consultare i file aziendali. Tuttavia, l'assenza di punibilità dura solo per il tempo della connessione. Se interrompe la connessione e ne stabilisce una nuova, è colpevole del reato. A nostro avviso, questa assenza di punibilità è chiaramente una scappatoia descritta in modo improprio, poiché probabilmente le parti non hanno previsto questa possibilità al momento della stesura del testo. 17

C. Illegalità

Per essere punibile, l'autore deve aver agito senza diritto. A tal fine, occorre innanzitutto stabilire se il sistema informatico è pubblico, ossia aperto a tutti, 18

o se l'accesso ad esso è limitato, o una combinazione di entrambi. Se il sistema informatico è pubblico, l'accesso non può in alcun caso essere illecito e l'eventuale reato è escluso. Se invece l'accesso a tutto o a parte del sistema informatico è limitato, l'accesso non autorizzato è punibile.

- 19 È il legittimo proprietario del sistema informatico a stabilire chi è autorizzato ad accedere a quale parte del sistema informatico. Ciò significa che sono punibili non solo coloro che non sono stati autorizzati ad accedere al sistema informatico, ma anche coloro che sono stati autorizzati ad accedere a una parte del sistema informatico ma che accedono a un'altra parte del sistema informatico a cui non è stato concesso l'accesso. Non sono invece punibili le persone che sono state autorizzate ad accedere al sistema informatico dal suo legittimo proprietario e che rispettano le limitazioni di accesso.
- 20 Il legittimo proprietario di un sistema informatico non è sempre il suo amministratore. Ciò è particolarmente vero per i sistemi informatici di medie e grandi dimensioni. In queste situazioni, la gestione del sistema informatico è delegata dal legittimo proprietario a un amministratore terzo. Questo amministratore può essere una persona fisica o una persona giuridica. In entrambi i casi, il legittimo proprietario del sistema informatico autorizza l'amministratore ad accedere al sistema per svolgere i propri compiti. L'amministratore, quindi, non ha accesso non autorizzato al sistema informatico finché lo fa per svolgere i suoi compiti. L'accesso è invece non autorizzato quando ha un altro scopo, come la consultazione di informazioni private o riservate non destinate all'amministratore.
- 21 Quando la gestione di un sistema informatico è delegata a una società, tutte le persone fisiche responsabili di questo compito all'interno della società sono autorizzate ad accedervi. Tuttavia, ciò non vale per le persone fisiche all'interno dell'entità giuridica a cui non è stato assegnato questo compito. Se queste persone accedono al sistema informatico, lo fanno senza diritto, poiché non lo fanno per svolgere il compito affidato alla persona giuridica.
- 22 Una persona specificamente incaricata di testare la sicurezza del sistema informatico che riesce ad accedere al sistema informatico aggirando le misure di protezione predisposte non agisce illegalmente, in quanto è stata autorizzata a farlo dal suo beneficiario.

D. Intenzione

L'accesso illegale è intenzionale. L'intenzione deve riguardare tutti gli 23
elementi oggettivi della violazione. L'autore deve quindi essere consapevole di
accedere senza diritto a un sistema informatico e avere la volontà di farlo. È
sufficiente una possibile frode. Se l'autore sospetta di accedere in tutto o in
parte a un sistema informatico a cui non dovrebbe avere accesso, ma
stabilisce comunque una connessione, è colpevole di accesso illecito. Se
invece l'autore commette un errore di manipolazione e stabilisce suo
malgrado una connessione non autorizzata, non c'è dolo e il reato non viene
commesso.

La legge punisce solo la creazione di un accesso illegale e non il fatto di 24
mantenere l'accesso contro la volontà del titolare del diritto. Di conseguenza,
una persona che accede inavvertitamente a un sistema informatico ma, una
volta collegata, ne esplora il contenuto, non è punibile.

Se l'autore crede erroneamente che il sistema informatico a cui sta accedendo 25
sia pubblico, o se crede erroneamente di avere il diritto di accedervi per
qualche altro motivo, è in errore sui fatti.

IV. ELEMENTI COSTITUTIVI AGGIUNTIVI FACOLTATIVI

Durante la stesura della Convenzione sulla criminalità informatica, la 26
maggioranza delle Parti voleva rendere la pirateria un reato puro e semplice.
Altre, invece, erano contrarie a una criminalizzazione generale dell'hacking, in
quanto la semplice intrusione non provoca necessariamente un danno e, in
alcuni casi, gli atti di hacking consentono addirittura di scoprire e colmare le
lacune della sicurezza. Per tenere conto di queste considerazioni, e dato che
le legislazioni nazionali di molti Paesi contenevano già disposizioni che
punivano l'hacking in varie forme, alle Parti è stata data la possibilità di
limitare la punibilità dell'accesso illegale richiedendo il soddisfacimento di
uno o più elementi costitutivi aggiuntivi.

A. Accesso in violazione delle misure di sicurezza

La Convenzione sulla criminalità informatica offre innanzitutto alle Parti la 27
possibilità di punire l'accesso illecito solo se commesso in violazione delle
misure di sicurezza. La Repubblica Ceca, la Finlandia, la Germania, il

Giappone, la Lituania, il Perù, la Repubblica Slovacca e la Svizzera si sono avvalsi di questa possibilità.

- 28 Questo requisito aggiuntivo significa che il sistema informatico deve essere protetto dall'accesso non autorizzato. In altre parole, se l'autore accede senza autorizzazione a un sistema informatico non protetto, non è punibile.
- 29 Il concetto di misure di sicurezza deve essere inteso in senso ampio. Esso comprende sia le misure di sicurezza fisiche che quelle virtuali. Per quanto riguarda le misure di sicurezza fisiche, il sistema informatico può, ad esempio, essere collocato in una stanza chiusa a chiave a cui si può accedere solo con una chiave, un badge magnetico, un'impronta digitale, una scansione della retina o un'impronta vocale. Le misure di sicurezza virtuali possono includere protezione firewall, codici PIN, password o doppia o addirittura tripla autenticazione.
- 30 Se l'autore del reato non riesce ad aggirare le misure di sicurezza, o se decide spontaneamente di interrompere la sua attività prima di averle superate, si può prevedere un solo tentativo. Ciò pone tuttavia un problema, in quanto l'art. 11 § 2 CCC non impone alle Parti di punire il tentativo di accesso illegale. Ogni Stato è quindi libero di trattare questo aspetto come meglio crede, con il risultato che questo comportamento potrebbe non essere affatto punibile, a seconda della legislazione nazionale degli Stati contraenti.
- 31 Un'altra possibilità offerta alle Parti è quella di richiedere che l'autore del reato abbia agito con uno scopo particolare. Diversi Stati si sono avvalsi di questa possibilità.
- 32 Gli Stati Uniti d'America hanno deciso di richiedere che l'autore abbia agito allo scopo di ottenere dati. Sebbene alle Parti sia stata concessa questa possibilità, il suo utilizzo è deplorabile perché svuota la norma di gran parte della sua sostanza. Questa disposizione è stata concepita specificamente per punire gli atti degli hacker che accedono ai sistemi informatici per spavalderia, senza tuttavia essere interessati ai dati in essi contenuti. La richiesta di questa finalità specifica sembra quindi contraria allo spirito della disposizione.
- 33 Il Belgio, da parte sua, ha dichiarato che l'accesso illecito è considerato reato solo se commesso con intento fraudolento o doloso. L'intento fraudolento sembra riferirsi al desiderio di ottenere un vantaggio indebito per sé o per

un'altra persona. Per quanto riguarda il dolo, probabilmente si riferisce all'intenzione di arrecare danno a un'altra persona in qualsiasi forma.

Il Principato di Andorra e la Repubblica Slovacca hanno deciso di perseguire l'accesso illecito solo se commesso allo scopo di ottenere dati senza diritto, danneggiarli (solo nel caso del Principato di Andorra) o con un altro intento criminale. Questa formulazione mira a evitare che gli autori del reato sfuggano alla condanna perché perseguono uno scopo diverso dall'ottenimento o dal danneggiamento dei dati. A nostro avviso, tuttavia, deve essere interpretata alla luce degli scopi speciali elencati nell'art. 2 del Codice penale, e deve essere simile sia in termini di scopo perseguito dall'autore del reato che di intensità criminale. Il 1° gennaio 2021, il Codice penale slovacco è stato modificato e la Riserva della Repubblica slovacca è stata adattata. La sezione 247 è stata riformulata. Nella sua forma semplice, questa disposizione non richiede più alcuno scopo speciale (§ 247 par. 1). D'altro canto, il § 247 par. 2 prevede una forma qualificata nel caso in cui l'autore del reato provochi un danno considerevole. 34

Infine, il Canada ha indicato che perseguirà l'accesso illecito solo se commesso con premeditazione. Quest'ultimo concetto è particolarmente impreciso e di conseguenza crea una notevole incertezza nella legge. Inoltre, sembra sovrapporsi alla nozione di dolo. A nostro avviso, quindi, deve essere interpretato in modo restrittivo. 35

Il Cile ha inizialmente formulato una riserva identica a quella del Canada. Tuttavia, ha modificato la propria legislazione nel 2022. Nella nuova versione, l'accesso illecito è punibile se commesso intenzionalmente. Non è più richiesto il dolo speciale. Tuttavia, quando l'accesso illecito è commesso allo scopo di ottenere o utilizzare i dati contenuti nel sistema informatico, la pena è aumentata. 36

C. Un sistema informatico collegato a un altro sistema informatico

Infine, la Convenzione sulla criminalità informatica consente alle Parti di limitare la punibilità dell'accesso illecito alle connessioni stabilite senza diritto con un sistema informatico attraverso un altro sistema informatico. Avvalendosi di questa possibilità, le Parti possono escludere i casi in cui 37

l'autore del reato acceda fisicamente al sistema informatico preso di mira, senza passare attraverso una rete.

- 38 Gli unici Stati che si sono avvalsi di questa possibilità sono la Repubblica Slovacca e il Giappone. Il Codice penale slovacco è stato successivamente modificato. La nuova formulazione del § 247, entrata in vigore il 1° gennaio 2021, non prevede più questo requisito nella sua versione attuale, pertanto la riserva della Repubblica Slovacca è stata adattata.

V. CONFRONTO CON IL DIRITTO SVIZZERO

- 39 Secondo il diritto svizzero, la pirateria informatica è punita dall'articolo 143^{bis} del Codice penale svizzero. Questa disposizione punisce l'accesso non autorizzato al sistema informatico di un'altra persona, appositamente protetto dall'accesso, per mezzo di un dispositivo di trasmissione dati. Tuttavia, questa disposizione non soddisfa i requisiti dell'art. 2 CCC sotto tre aspetti.
- 40 In primo luogo, la Convenzione non distingue tra sistemi informatici. Essa protegge l'integrità di tutti i sistemi informatici, indipendentemente dalla loro ubicazione. L'articolo 143^{bis} cpv. 1 del Codice penale, invece, incrimina solo l'accesso non autorizzato a un sistema informatico "appartenente a un'altra persona". Poiché questa disposizione si trova nel Titolo 2 del Codice Penale, ossia i reati contro la proprietà, questa formulazione deve essere interpretata con riferimento ai diritti reali. Il sistema informatico deve quindi appartenere a una persona diversa dall'autore. Se l'autore è proprietario o comproprietario del sistema informatico, questo elemento costitutivo non è soddisfatto perché non appartiene a qualcun altro. Pertanto, se sono state aperte diverse sessioni nello stesso sistema informatico, l'autore, che è il (co)proprietario del sistema informatico, che accede a una sessione diversa dalla propria non è punibile. La maggior parte dei giuristi, invece, ritiene che "appartenere a un'altra persona" debba essere inteso nel senso che una persona diversa dall'autore è autorizzata ad accedere e utilizzare il sistema informatico o un sottosistema informatico. Tale interpretazione, tuttavia, renderebbe superflua la nozione di "appartenenza a un'altra persona" rispetto all'elemento costitutivo dell'accesso illecito. Il motivo per cui il legislatore ha menzionato questi due elementi separatamente è che si tratta di due concetti che devono essere analizzati indipendentemente l'uno dall'altro. Per coerenza con la Convenzione, il termine "altri" di cui all'art. 143^{bis} cpv. 1 c.p. dovrebbe quindi essere eliminato.

L'art. 143^{bis} cpv. 1 del Codice penale richiede che l'autore del reato abbia avuto accesso al sistema informatico per mezzo di un dispositivo di trasmissione dati. Ciò significa, ad esempio, che un autore che approfitta dell'assenza della vittima per entrare nel suo ufficio e collegarsi direttamente al suo computer non è colpevole di accesso non autorizzato a un sistema informatico, poiché non sta utilizzando un dispositivo di trasmissione dati. L'articolo 2 § 2 del Codice penale consente alle Parti di limitare l'azione penale all'accesso illecito commesso per mezzo di un sistema informatico collegato a un altro sistema informatico. Tuttavia, la Svizzera non ha dichiarato di volersi avvalere di questa possibilità. Di conseguenza, l'elemento costitutivo dell'accesso per mezzo di un dispositivo di trasmissione dati dovrebbe essere eliminato. 41

Infine, l'articolo 143^{bis} del Codice penale prevede un reato perseguito solo a querela di parte. Tuttavia, se un reato è perseguito solo a querela di parte, l'autorità penale non può assumersi la giurisdizione. Poiché esiste un conflitto di dottrina sul fatto che una denuncia presentata nello Stato richiedente sia sufficiente per attuare la cooperazione internazionale, sarebbe prudente perseguire d'ufficio l'accesso indebito a un sistema informatico. 42

Alla luce di quanto precede, si deve concludere che il diritto svizzero non è conforme all'articolo 2 CPC. L'articolo 143^{bis} del Codice penale svizzero dovrebbe pertanto essere modificato. 43

I concetti tecnici informatici contenuti in questo contributo sono stati redatti con l'aiuto di Yannick Jacquy, responsabile ICT con diploma federale. Desideriamo ringraziarlo calorosamente per la sua assistenza.

BIBLIOGRAFIA

Dupuis Michel / Geller Bernard / Monnier Gilles / Moreillon Laurent / Piguet Christophe / Bettex Christian / Stoll Daniel (éditeurs), Code pénal - Petit commentaire, 2. éd., Bâle 2017

Pfister Christa, Hacking in der Schweiz, Diss., Zürich, 2008

Schmid Niklaus, Computer- sowie Check- und Kreditkartenkriminalität, Zurich 1994

Schwarzenegger Christian, Die internationale Harmonisierung des Computer- und Internetstrafrechts durch die Convention on Cybercrime, in : Strafrecht, Strafprozessrecht und Menschenrechte, Festschrift Trechsel, Zurich 2002

Stratenwerth Günter / Bommer Felix, Schweizerisches Strafrecht, Besonderer Teil I: Straftaten gegen Individualinteressen, 8. éd., Berne, 2022

Trechsel Stefan / Cramer Dean, in : Trechsel Stefan / Pieth Mark (éditeurs), Schweizerisches Strafgesetzbuch, Praxiskommentar, 4. éd., Zurich 2021

Weissenberg Philippe, in : Niggli Marcel Alexander / Wiprächtiger Hans (éditeurs), Basler Kommentar, Strafrecht II, 4. éd., Bâle 2018

I MATERIALI

Conseil de l'Europe, Explanatory Report to the Convention on Cybercrime, Budapest 23.11.2001, disponible sous <https://rm.coe.int/16800cce5b>, visité le 21.1.2024 (cité : Rapport explicatif de la Convention sur la cybercriminalité)

Message concernant la modification du code pénal suisse et du code pénal militaire (Infractions contre le patrimoine et faux dans les titres) ainsi que la modification de la loi fédérale sur l'approvisionnement économique du pays (Dispositions pénales) du 24 avril 1991, FF 1991 II 933, disponible sous https://www.fedlex.admin.ch/eli/fga/1991/2_969_933_797/fr, visité le 21.1.2024

ATTENZIONE: Questa versione del commentario è una traduzione automatica dell'originale. Il commentario originale è in francese. La traduzione è stata effettuata con www.deepl.com. Solo la versione originale fa fede. La forma tradotta del commentario non può essere citata

COMMENTO SU

Art. 3 CCC (Convenzione sulla cibercriminalità [Cybercrime Convention])

Un commentario di Jérémie Müller

CITAZIONE SUGGERITA

Jérémie Müller, Commentario all'art. 3 CCC, in: Damian K. Graf (a cura di), Commentario online alla Convenzione sulla cibercriminalità (Cybercrime Convention)

Breve citazione: OK-Müller, art. 3 CCC N. XXX.

Art. 3 Intercettazione illecita

Le Parti adottano le misure legislative e di altra natura necessarie per definire come reato, nel loro diritto interno, l'intercettazione intenzionale e illecita, eseguita con strumenti tecnici, di trasmissioni non pubbliche di dati informatici a, da o all'interno di un sistema informatico, incluse le emissioni elettromagnetiche emesse da un sistema informatico in cui sono salvati tali dati informatici. Le Parti possono esigere che il reato sia commesso con intento illegale oppure

in relazione a un sistema informatico collegato a un altro sistema informatico.

STRUTTURA

I. Generalità.....	46
II. Beni giuridicamente protetti	46
III. Elementi costitutivi di base.....	46
A. Dati informatici	46
B. Trasmissione non pubblica.....	47
1. Il concetto di trasmissione	47
2. Natura non pubblica	48
C. Il caso particolare delle emissioni elettromagnetiche.....	48
D. Intercettazione con mezzi tecnici	50
E. Illecito	51
F. Intenzione	52
IV. Elementi costitutivi aggiuntivi facoltativi	52
A. Lo scopo di ottenere dati informatici o un altro scopo speciale.....	53
B. Un sistema informatico collegato a un altro sistema informatico.	53
V. Confronto con il diritto svizzero	54
Bibliografia	55
I Materiali	56

I. GENERALITÀ

- 1 Per garantire una protezione giuridica completa, l'accesso illecito doveva essere integrato dall'intercettazione illecita. Come abbiamo visto in precedenza (cfr. art. 2 N. 9ss), l'accesso illecito punisce l'intrusione illegale nel sistema informatico e la consultazione da parte di persone non autorizzate dei dati ivi memorizzati. L'intercettazione illecita, invece, punisce la violazione della riservatezza dei dati che circolano all'interno del sistema informatico, nonché dei dati scambiati tra il sistema informatico e il mondo esterno.

II. BENI GIURIDICAMENTE PROTETTI

- 2 Questa disposizione tutela il diritto alla riservatezza dei dati trasmessi. Il reato rappresenta la stessa violazione del diritto alla segretezza delle comunicazioni della tradizionale intercettazione e registrazione delle conversazioni telefoniche tra privati. L'articolo 3 CCC incorpora la garanzia del diritto al rispetto della corrispondenza contenuta nell'articolo 8 CEDU e la applica a tutte le forme di trasferimento elettronico di dati, sia per telefono, fax, e-mail o file.

III. ELEMENTI COSTITUTIVI DI BASE

A. Dati informatici

- 3 Ai sensi dell'art. 1 lett. b CCC, per "dati informatici" si intende qualsiasi rappresentazione di fatti, informazioni o concetti in una forma idonea al trattamento in un sistema informatico, compreso un programma idoneo a far eseguire una funzione a un sistema informatico. Il concetto di dati informatici è quindi molto ampio e comprende in particolare tutte le lettere, i simboli o i codici di programmazione che possono essere inseriti, elaborati e memorizzati da un sistema informatico.
- 4 Per maggiori dettagli su questo concetto, si rimanda a quanto scritto sull'art. 1 CCC.

B. Trasmissione non pubblica

1. Il concetto di trasmissione

Contrariamente a quanto potrebbe suggerire l'etimologia del termine "trasmissione", la nozione di trasmissione di cui all'art. 3 initio CCC non si riferisce solo agli scambi a distanza tra due dispositivi. Come suggeriscono le preposizioni "a", "da" o "all'interno" di un sistema informatico, riguarda tutti i dati in circolazione. Gli unici dati che non rientrano in questo concetto sono quelli memorizzati in modo permanente su un supporto, come un disco rigido, una chiave USB o un DVD.

La trasmissione di dati "all'interno" di un sistema informatico riguarda i dati che circolano tra la scheda madre, il processore, la scheda grafica, lo schermo del computer o la stampante. Si estende anche ai dati memorizzati nella memoria ad accesso casuale del sistema informatico, poiché questi dati non vengono memorizzati in modo permanente in questa memoria, ma vi rimangono solo per pochi istanti prima di continuare a circolare nel sistema informatico.

La trasmissione di dati "a" o "da" un sistema informatico presuppone che il destinatario o il mittente dei dati sia un sistema informatico, mentre l'altro può essere un essere umano o un sistema informatico.

Nel caso di trasmissione di dati da un essere umano "a" un sistema informatico, l'obiettivo è che l'essere umano inserisca i dati nel sistema informatico, ad esempio utilizzando una tastiera, un mouse o un joystick. Al contrario, la trasmissione di dati a un essere umano "dal" sistema informatico è intesa come la restituzione di dati dal sistema informatico all'essere umano attraverso la visualizzazione dei dati su uno schermo o la stampa di un documento su una stampante.

Infine, la trasmissione di dati tra due sistemi informatici avviene sia "verso" che "da" un sistema informatico. Questo è il caso in particolare di uno scambio tra un computer e un server, tra due computer o tra un computer e uno smartphone. Non importa se i due sistemi informatici appartengono alla stessa persona o a persone diverse. Non importa nemmeno il modo in cui i dati vengono trasmessi. I dati possono essere scambiati tramite una connessione cablata o wireless (WiFi, NFC, Bluetooth, onde radio, ecc.).

- 10 Gli elementi di cui sopra dimostrano che il concetto di trasmissione è molto ampio. Per limitare la portata di questa disposizione, l'articolo 3 del Codice penale consente alle Parti di limitare l'azione penale all'intercettazione illecita di dati trasmessi tra due sistemi informatici collegati a distanza.

2. Natura non pubblica

- 11 L'articolo 3 del Codice penale riguarda solo le trasmissioni non pubbliche. La natura non pubblica riguarda la trasmissione e non i dati trasmessi. È quindi irrilevante che i dati trasmessi siano pubblici o privati. Solo la natura della trasmissione è determinante.
- 12 A nostro avviso, una trasmissione non è pubblica quando è limitata a un certo numero di persone o a persone specifiche. È il caso, ad esempio, della trasmissione di una presentazione in videoconferenza che può essere seguita solo da un numero limitato di partecipanti, o di film resi disponibili solo agli abbonati da una società di streaming.
- 13 Il concetto di trasmissione non pubblica non significa, tuttavia, che la trasmissione debba avvenire su una rete non pubblica. La trasmissione può avvenire tramite una rete pubblica; è semplicemente necessario che tale trasmissione sia limitata a un numero specifico di persone.
- 14 Per limitare una trasmissione a un numero specifico di persone, è necessario adottare misure tecniche. Tuttavia, tali misure di sicurezza non devono essere particolarmente avanzate. È sufficiente un sistema per verificare che la persona che desidera accedere alla trasmissione sia una delle persone autorizzate. Ad esempio, può essere necessario seguire un link inviato via e-mail, inserire un codice fornito in precedenza o identificarsi tramite un nome utente e una password.

C. Il caso particolare delle emissioni elettromagnetiche

- 15 Quando la Convenzione sulla criminalità informatica è stata redatta tra l'aprile 1997 e il dicembre 2000, gli esperti hanno voluto anticipare gli sviluppi tecnologici. L'intercettazione illegale non è stata quindi limitata alla sola trasmissione di dati, ma è stata estesa alle emissioni elettromagnetiche.
- 16 Per capire come funziona l'intercettazione delle emissioni elettromagnetiche, è importante ricordare che i dati informatici sono espressi in linguaggio

binario come una successione di "0" e "1". Questa è la forma in cui i sistemi informatici elaborano i dati. Da un punto di vista microtecnico, è quindi necessario generare impulsi elettrici diversi per uno "0" e un "1". A questo servono i transistor. In generale, i sistemi informatici sono costituiti da una moltitudine di transistor. Questi transistor permettono alla tensione che attraversa i componenti elettronici del sistema informatico di variare da bassa ad alta, a seconda che il bit da elaborare sia uno "0" o un "1". Queste innumerevoli variazioni di tensione creano un campo elettromagnetico che si propaga intorno al sistema informatico. Ciò consente a una persona nelle vicinanze, dotata di un dispositivo adeguato, di captare questo flusso, di riconvertirlo in "0" e "1" e di ricostruire così i dati informatici elaborati dal sistema informatico.

Per gli esperti, l'arsenale giuridico sembrava incompleto se si limitava a punire 17 l'intercettazione dei dati trasmessi a, da o da un sistema informatico, senza punire contemporaneamente la cattura delle onde elettromagnetiche emesse da un sistema informatico. Nel mondo reale, ciò sarebbe equivalso a punire l'intercettazione di una persona nel suo appartamento per mezzo di un microfono, lasciando impunita l'intercettazione delle conversazioni di quella persona da dietro la porta d'ingresso dell'appartamento.

In particolare, è opportuno ricordare che all'epoca della stesura della 18 Convenzione erano molto diffusi i fax. Questo dispositivo inviava dati non codificati a una frequenza e a un'intensità elettrica che rendevano abbastanza facile captarli e poi ricostruirli in un linguaggio comprensibile. Gli esperti hanno certamente individuato una falla nella sicurezza che poteva essere sfruttata dai criminali informatici, il che li ha portati a includere la cattura di onde elettromagnetiche nell'elenco dei reati punibili.

Nel corso degli anni, il fax è quasi completamente scomparso. Oggi la cattura 19 delle onde elettromagnetiche è diventata molto marginale, se non inesistente, a causa delle difficoltà tecniche che comporta la cattura di questi segnali. I cavi elettrici utilizzati oggi in informatica sono molto più isolati rispetto alla fine degli anni '90 e gli impulsi elettrici sono molto più deboli. Allo stesso tempo, la quantità di dati scambiati ogni secondo è esplosa. Di conseguenza, oggi è praticamente impossibile catturare le onde magnetiche da una singola sorgente e ricostruirle in dati intelligibili.

- 20 Tuttavia, quando è stato redatto il testo della Convenzione, gli esperti non potevano prevedere la direzione in cui si sarebbe evoluta la tecnologia. Ecco perché questo comportamento - anche se ormai aneddótico - è incluso nell'elenco dei reati di cui all'art. 3 CCC.

D. Intercettazione con mezzi tecnici

- 21 L'articolo 3 del Codice penale si applica solo all'intercettazione di dati con mezzi tecnici. La sottrazione fisica di dati, in particolare il furto di una chiave USB inviata per posta o il furto di un computer portatile acceso e sbloccato in un luogo pubblico, non sono pertanto punibili ai sensi di questa disposizione.
- 22 L'intercettazione di cui all'articolo 3 del Codice penale può essere diretta o indiretta. L'autore del reato intercetta i dati direttamente quando accede al sistema informatico stesso. La forma più semplice è l'installazione di un cavallo di Troia nel sistema informatico, che consente all'autore del reato di accedervi. L'autore può anche utilizzare una backdoor o sfruttare una falla di sicurezza. Tutte queste tecniche consentono all'aggressore di conoscere in tempo reale i dati che circolano nel sistema informatico.
- 23 Si parla di intercettazione indiretta quando l'autore del reato intercetta il flusso di dati scambiati tra due dispositivi. È il caso, ad esempio, della cattura del flusso di dati tra un dispositivo e un terminale Wifi a cui è collegato. All'interno di una rete locale (LAN), il malintenzionato può anche usurpare l'indirizzo MAC di un sistema informatico al momento della trasmissione per far sì che i pacchetti di dati vengano inviati al sistema il cui indirizzo è stato usurpato. Un'altra tecnica è il port mirroring. Inizialmente, lo scopo di questo sistema è controllare i dati scambiati all'interno di una rete. A tal fine, una copia di tutti i dati che passano attraverso uno switch di rete viene inviata a un sistema di controllo informatico. Tuttavia, prendendo il controllo dello switch di rete, l'autore del reato può reindirizzare i dati copiati al proprio sistema informatico, che gli consente di accedere a tutti i dati scambiati sulla rete.
- 24 Il concetto di "mezzi tecnici" utilizzato dalle parti è molto ampio e impreciso. Non è neppure accompagnato da un elenco esemplificativo. Questa scelta è senza dubbio volta a consentire alla norma di adattarsi più facilmente alle innovazioni tecnologiche. In ogni caso, i dispositivi interessati sono quelli che consentono di ascoltare, controllare o monitorare il contenuto delle comunicazioni. Si tratta di dispositivi tecnici collegati alle linee di

trasmissione, nonché di dispositivi per la raccolta e la registrazione di comunicazioni senza fili. Tuttavia, i mezzi tecnici di cui all'art. 3 CCC non si limitano all'hardware. Sono inclusi anche software, password e altri codici.

E. Illecito

Per essere punibile, l'autore deve aver agito senza diritto. È il legittimo proprietario dei dati a stabilire chi è autorizzato ad accedervi. Tutte le persone che non sono state autorizzate a consultare i dati sono quindi punibili. Non sono invece punibili le persone che sono state autorizzate ad accedere ai dati dal legittimo proprietario o che sono autorizzate a farlo in virtù della legge o di un contratto. 25

Le leggi nazionali contengono eccezioni alla garanzia di riservatezza dei dati. In particolare, consentono ai servizi di intelligence di accedere a dati non destinati a loro. Inoltre, consentono alle autorità giudiziarie di monitorare i flussi di dati in tempo reale nell'ambito di un'indagine penale. Queste intercettazioni non sono illegali, purché siano effettuate nel rigoroso rispetto delle disposizioni di legge in vigore. Tuttavia, la sorveglianza può essere effettuata solo in casi gravi e deve essere soggetta a un successivo controllo giudiziario. 26

L'intercettazione dei dati non è considerata illegale nemmeno quando è autorizzata contrattualmente. Ciò avviene in particolare quando l'amministratore del sistema informatico è responsabile della manutenzione. In questo caso, non è punibile se intercetta i dati di cui ha bisogno per svolgere il suo lavoro, perché è stato autorizzato dal titolare del diritto. Allo stesso modo, la persona responsabile del monitoraggio di una rete non è punibile se intercetta i dati ottenuti attraverso un uso corretto, come il port mirroring. Quando invece tali persone sfruttano le possibilità tecniche a loro disposizione per intercettare dati non necessari allo svolgimento del loro lavoro, agiscono illegalmente. 27

Nel contesto dei rapporti di lavoro, l'intercettazione lecita dei dati è concepibile, ma soggetta a condizioni restrittive. In generale, la Corte europea dei diritti dell'uomo ha stabilito che le comunicazioni private dei dipendenti sono protette dall'articolo 8 della CEDU. La sorveglianza da parte del datore di lavoro è quindi concepibile solo se il dipendente è stato informato del fatto che le sue comunicazioni sono monitorate, della natura e della portata della 28

sorveglianza e del grado di intrusione nella sua vita privata e nella sua corrispondenza. Se il datore di lavoro rispetta queste condizioni, l'intercettazione dei dati dei dipendenti è lecita.

- 29 In origine, l'art. 3 CCC non era destinato a sanzionare le comuni pratiche commerciali volte a ottenere informazioni sugli utenti. Dall'entrata in vigore della Convenzione sulla criminalità informatica, le pratiche commerciali si sono notevolmente evolute e le informazioni che le imprese commerciali cercano di ottenere per indirizzare la loro pubblicità sono sempre più importanti. Di conseguenza, la legislazione nazionale ha rafforzato in modo significativo la protezione dei dati e dei consumatori. È quindi diventato molto comune che i siti web debbano ottenere il consenso degli utenti di Internet prima di raccogliere dati su di loro, in particolare utilizzando i "cookie". Senza il consenso del legittimo proprietario, la raccolta di tali dati potrebbe costituire un'intercettazione illegale.

F. Intenzione

- 30 L'intercettazione illecita è intenzionale. L'intenzione deve riguardare tutti gli elementi oggettivi del reato. L'autore del reato deve quindi essere consapevole di ottenere dati in modo improprio e avere la volontà di farlo. È sufficiente una possibile frode. Nella sua forma semplice, lo scopo perseguito dall'autore del reato è irrilevante.

IV. ELEMENTI COSTITUTIVI AGGIUNTIVI FACOLTATIVI

- 31 L'articolo 3 del Codice penale consente alle Parti di limitare la punibilità a determinati atti specifici aggiungendo uno o due degli elementi costitutivi elencati alla fine di questa disposizione.
- 32 A seconda del modo in cui l'intercettazione illecita viene trascritta nel diritto nazionale, questo reato può essere strettamente legato all'accesso illecito (articolo 2 del Codice penale). Poiché alcuni Stati hanno scelto di limitare la punizione dell'accesso illecito ai casi commessi con dolo specifico o per mezzo di un sistema informatico collegato a un altro sistema informatico, è stato necessario consentire a tali Stati di limitare l'intercettazione illecita a questi stessi casi.

A. Lo scopo di ottenere dati informatici o un altro scopo speciale

La prima possibilità offerta alle Parti è quella di richiedere che l'autore del reato abbia agito con uno scopo particolare. Diversi Stati si sono avvalsi di questa possibilità. 33

Canada, Giappone e Perù hanno indicato che perseguirebbero l'intercettazione illegale solo se commessa con intento criminale. Quest'ultimo concetto è particolarmente impreciso e di conseguenza crea una notevole incertezza nella legge. Inoltre, sembra sovrapporsi al concetto di dolo. A nostro avviso, quindi, deve essere interpretato in modo restrittivo. 34

Il Cile ha inizialmente formulato una riserva identica a quella di Canada, Giappone e Perù. Tuttavia, ha modificato la propria legislazione nel 2022. Nella nuova versione, l'intercettazione illecita non richiede più uno scopo speciale. 35

La Svizzera, da parte sua, ha dichiarato che perseguirà l'intercettazione illegale solo se l'autore ha agito in vista di un arricchimento illecito. 36

Mentre il Principato di Andorra, il Belgio, gli Stati Uniti d'America e la Repubblica Slovacca hanno dichiarato che avrebbero perseguito l'accesso illecito solo se l'autore avesse agito con uno scopo speciale, hanno rinunciato allo stesso requisito per l'intercettazione illecita. 37

B. Un sistema informatico collegato a un altro sistema informatico.

La Convenzione sulla criminalità informatica autorizza inoltre le Parti a limitare la punibilità dell'intercettazione illecita ai soli dati trasmessi tra due sistemi informatici collegati tra loro. Gli unici Stati che si sono avvalsi di questa possibilità sono il Giappone e il Perù. 38

Anche in questo caso, è sorprendente notare che la Repubblica Slovacca ha rifiutato di avvalersi di questa possibilità, nonostante avesse espressamente dichiarato che avrebbe perseguito l'accesso illecito solo se commesso per mezzo di un sistema informatico collegato a un altro sistema informatico. 39

V. CONFRONTO CON IL DIRITTO SVIZZERO

- 40 Nel suo messaggio sull'approvazione e l'attuazione della Convenzione del Consiglio d'Europa sulla criminalità informatica, il Consiglio federale ha riconosciuto che "il diritto penale svizzero non dispone di norme corrispondenti all'art. 3 della Convenzione, ma diverse norme penali offrono una protezione parziale". A suo avviso, si tratta di una combinazione degli articoli 143, 143^{bis} e 321^{ter} del Codice penale svizzero. In realtà, le cose non stanno affatto così.
- 41 L'articolo 143^{bis} del Codice penale prevede come reato solo l'intrusione in un sistema informatico, non l'intercettazione di dati.
- 42 L'articolo 321^{ter} del Codice penale è un reato puramente penale, poiché può essere commesso solo da un dipendente di un'azienda che fornisce un servizio postale o di telecomunicazione.
- 43 Per quanto riguarda l'art. 143 del Codice penale svizzero, si tratta della disposizione che più si avvicina all'art. 3 del Codice penale. Per conformarsi ai requisiti della Convenzione, tuttavia, questa disposizione dovrebbe essere modificata sotto quattro aspetti.
- 44 In primo luogo, i beni giuridici tutelati dalle due disposizioni sono diversi. L'articolo 3 del Codice penale tutela la riservatezza dei dati trasmessi, mentre l'articolo 143 del Codice penale tutela "il diritto del legittimo destinatario dei dati di disporne liberamente e secondo la sua volontà". Il diritto legale tutelato dall'articolo 143 del Codice penale svizzero dovrebbe quindi essere adattato.
- 45 In secondo luogo, l'articolo 3 del Codice penale prevede come reato l'intercettazione di trasmissioni non pubbliche, indipendentemente dal fatto che i dati trasmessi siano pubblici o meno. Tuttavia, l'articolo 143 del Codice penale svizzero punisce solo l'appropriazione indebita di dati appositamente protetti dall'accesso. Il furto di dati pubblici trasmessi in modo non pubblico non è quindi coperto dall'articolo 143 del Codice penale. Nella pratica, tuttavia, questo è il caso più comune, poiché i dati trasmessi elettronicamente non sono generalmente protetti in modo speciale contro l'accesso.
- 46 In secondo luogo, l'articolo 143 del Codice Penale protegge solo il diritto di disporre dei dati. I dati informatici non hanno sempre un valore intrinseco. Richiedere uno scopo di arricchimento senza causa equivale quindi a escludere la tutela penale in tutti i casi in cui l'autore sottrae dati privi di

valore. In considerazione del bene giuridicamente protetto, questo elemento costitutivo dovrebbe essere eliminato.

Infine, l'articolo 3 CCC non si limita alle sole trasmissioni non pubbliche, ma include anche le emissioni elettromagnetiche. Tuttavia, queste non sono protette dall'articolo 143 del Codice Penale. È quindi opportuno aggiungerle. 47

Per tutti questi motivi, si deve concludere che la legge svizzera non è conforme all'articolo 3 CCC e deve quindi essere adattata. 48

I concetti tecnici informatici contenuti in questo contributo sono stati redatti con l'aiuto di Yannick Jacquey, ICT Manager con diploma federale. Desideriamo ringraziarlo calorosamente per la sua assistenza.

BIBLIOGRAFIA

Oberholzer Niklaus, in: Niggli Marcel Alexander / Wiprächtiger Hans (éditeurs), Basler Kommentar, Strafrecht II, 4. éd., Bâle 2018

Schmid Niklaus, Computer- sowie Check- und Kreditkartenkriminalität, Zurich 1994

Schwarzenegger Christian, Die internationale Harmonisierung des Computer- und Internetstrafrechts durch die Convention on Cybercrime, in : Strafrecht, Strafprozessrecht und Menschenrechte, Festschrift Trechsel, Zurich 2002

Treccani Jean, Interceptions électroniques, in : Plus de sécurité, moins de liberté, les techniques d'investigation et de preuve en question, Zurich et Coire 2003

Trechsel Stefan / Cramer Dean, in : Trechsel Stefan / Pieth Mark (éditeurs), Schweizerisches Strafgesetzbuch, Praxiskommentar, 4. éd., Zurich 2021

Trechsel Stefan / Lehmkuhl Marianne Johanna , in : Trechsel Stefan / Pieth Mark (éditeurs), Schweizerisches Strafgesetzbuch, Praxiskommentar, 4. éd., Zurich 2021

Weissenberg Philippe, in: Niggli Marcel Alexander / Wiprächtiger Hans (éditeurs), Basler Kommentar, Strafrecht II, 4. éd., Bâle 2018

I MATERIALI

Conseil de l'Europe, Explanatory Report to the Convention on Cybercrime, Budapest 23.11.2001, disponible sous <https://rm.coe.int/16800cce5b>, visité le 21.1.2024 (cité : Rapport explicatif de la Convention sur la cybercriminalité)

Message concernant la modification du code pénal suisse et du code pénal militaire (Infractions contre le patrimoine et faux dans les titres) ainsi que la modification de la loi fédérale sur l'approvisionnement économique du pays (Dispositions pénales) du 24 avril 1991, FF 1991 II 933, disponible sous https://www.fedlex.admin.ch/eli/fga/1991/2_969_933_797/fr, visité le 21.1.2024

Message relatif à l'approbation et à la mise en œuvre de la Convention du Conseil de l'Europe sur la cybercriminalité, FF 2010 4275, disponible sous <https://www.fedlex.admin.ch/eli/fga/2010/813/fr>, visité le 21.1.2024

ATTENZIONE: Questa versione del commentario è una traduzione automatica dell'originale. Il commentario originale è in francese. La traduzione è stata effettuata con www.deepl.com. Solo la versione originale fa fede. La forma tradotta del commentario non può essere citata

COMMENTO SU

Art. 4 CCC (Convenzione sulla cibercriminalità [Cybercrime Convention])

Un commentario di Jérémie Müller

CITAZIONE SUGGERITA

Jérémie Müller, Commentario all'art. 4 CCC, in: Damian K. Graf (a cura di), Commentario online alla Convenzione sulla cibercriminalità (Cybercrime Convention)

Breve citazione: OK-Müller, art. 4 CCC N. XXX.

Art. 4 Attacco all'integrità dei dati

¹ Le Parti adottano le misure legislative e di altra natura necessarie per definire come reato, nel loro diritto interno, il danneggiamento, la cancellazione, il deterioramento, l'alterazione o la soppressione di dati informatici commessi intenzionalmente e illecitamente.

² Le Parti possono esigere che la condotta descritta al paragrafo 1 cagioni un danno grave.

STRUTTURA

I. Aspetti generali	59
II. Proprietà giuridicamente protetta.....	59
III. Elementi costitutivi di base.....	59
A. Dati informatici	59
B. Condotta punibile	60
1. Cancellare e cancellare i dati.....	60
2. Danneggiamento, deterioramento e alterazione dei dati.....	61
3. Modalità della Commissione	61
C. Illecito	62
D. Intenzione	63
IV. Elemento costitutivo aggiuntivo facoltativo	64
V. Confronto con il diritto svizzero	65
Bibliografia	65
I Materiali	66

I. ASPETTI GENERALI

Negli ultimi vent'anni, la società nel suo complesso è passata a un mondo digitale. Gran parte del commercio si svolge online, le transazioni finanziarie vengono effettuate tramite l'e-banking e le autorità, le imprese e i singoli cittadini conservano grandi quantità di informazioni su personal computer, server e persino cloud. Nonostante la portata dei cambiamenti già avvenuti, questa evoluzione non sembra affatto conclusa. Anzi, è molto probabile che la società continui a diventare ancora più digitale nei decenni a venire.

I documenti digitali stanno gradualmente sostituendo quelli cartacei. In linea con questa tendenza, i documenti in formato elettronico stanno diventando sempre più autorevoli.

Data la crescente importanza dei dati informatici nel mondo digitale, era giustificato proteggerli da atti dolosi. Mentre gli artt. 2 e 3 del CCC tutelano la riservatezza dei dati, l'art. 4 del CCC mira a garantire la protezione dell'integrità e della disponibilità dei dati.

II. PROPRIETÀ GIURIDICAMENTE PROTETTA

Lo scopo dell'art. 4 CCC è quello di fornire ai dati e ai programmi informatici una protezione simile a quella offerta ai beni materiali contro i danni intenzionali. Gli interessi giuridici tutelati da questa disposizione sono, da un lato, l'integrità dei dati e dei programmi informatici e, dall'altro, il corretto funzionamento o utilizzo dei dati e dei programmi informatici.

III. ELEMENTI COSTITUTIVI DI BASE

A. Dati informatici

Ai sensi dell'art. 1 lett. b CCC, "l'espressione 'dati informatici' indica qualsiasi rappresentazione di fatti, informazioni o concetti in una forma adatta all'elaborazione in un sistema informatico, compreso un programma progettato per far sì che un sistema informatico esegua una funzione". Il concetto di dati informatici è quindi molto ampio e comprende in particolare tutte le lettere, i simboli o i codici di programmazione che possono essere inseriti, elaborati e memorizzati da un sistema informatico.

- 6 Per maggiori dettagli su questo concetto, si rimanda a quanto scritto nel precedente art. 1 CCC.

B. Condotta punibile

- 7 Affinché un sistema informatico funzioni correttamente, i dati che elabora devono essere disponibili e accurati. Per garantire questi due aspetti, l'art. 4 del Codice penale elenca cinque condotte punibili. Punire la cancellazione e l'eliminazione dei dati ha lo scopo di proteggere la disponibilità dei dati. Il danneggiamento, il deterioramento o l'alterazione dei dati è punito per proteggere l'integrità dei dati. Questo elenco di comportamenti non è esaustivo. Tuttavia, copre tutti i possibili comportamenti dannosi.

1. Cancellare e cancellare i dati

- 8 In termini informatici, i dati sono espressi in linguaggio binario come una successione di "0" e "1". Questa è la forma in cui i dati vengono elaborati e memorizzati. Quando l'utente registra dei dati, il sistema informatico salva la serie di "0" e "1" corrispondente a questi dati in uno spazio vuoto del supporto di registrazione (ad es. disco rigido, DVD, chiave USB, ecc.). Per ritrovare questi dati quando l'utente ne ha bisogno, il sistema informatico dispone di una sorta di mappa che indica la posizione dei dati sul supporto.
- 9 L'eliminazione dei dati comporta la distruzione dei mezzi per localizzarli. I dati esistono ancora, ma l'utente non può più determinarne la posizione sul supporto e quindi non può più accedervi. Il sistema informatico ritiene che lo spazio sul supporto sia libero e quindi registra i nuovi dati al posto di quelli cancellati. L'unico modo per recuperare i dati cancellati è utilizzare un programma di recupero dati il più rapidamente possibile. Questo programma legge l'intero supporto e ricostruisce una mappa del supporto di registrazione per individuare i dati. In questo modo è possibile recuperare i dati prima che ne vengano registrati altri.
- 10 A differenza della cancellazione, la cancellazione dei dati è la distruzione permanente dei dati. I dati non esistono più sul supporto di registrazione. In linea di principio, non possono più essere recuperati.

2. Danneggiamento, deterioramento e alterazione dei dati

L'integrità dei dati è essenziale per il buon funzionamento dei sistemi informativi tanto quanto la disponibilità dei dati. La sua importanza è tale che è persino oggetto di uno standard ISO. L'integrità dei dati si riferisce all'affidabilità, all'accuratezza e alla completezza dei dati. In altre parole, i dati di cui è garantita l'integrità sono quelli che non sono stati modificati dopo la loro registrazione iniziale. Il concetto di integrità dei dati riguarda sia il contenuto dei dati che la loro forma. 11

Nel mondo reale, la nozione di integrità garantita dei dati può essere paragonata all'invio di un pacco per posta, dove si certifica che proviene realmente dal mittente indicato sul pacco, che è stato spedito alla data e nel luogo indicati dal timbro postale, che il pacco non è stato aperto, che il suo contenuto è quello inviato dal mittente e che nulla è stato rimosso o aggiunto al pacco dopo la spedizione. 12

In questo contesto, "danneggiamento" e "deterioramento" dei dati sono concetti che si sovrappongono. Descrivono danni negativi alla forma o al contenuto di dati o programmi. I dati danneggiati o deteriorati non sono più affidabili, accurati o completi. Non è quindi più possibile essere certi che provengano dal mittente da cui sembrano provenire, che siano effettivamente i dati inviati dal mittente e che nessun dato sia stato cancellato, aggiunto o modificato. 13

Per "alterazione" si intende una modifica dei dati esistenti. Tale modifica può riguardare sia la forma che il contenuto dei dati. Si tratta di un termine molto ampio che comprende tutte le azioni effettuate sui dati con l'aggiunta, la sostituzione o la cancellazione di uno o più elementi. 14

3. Modalità della Commissione

I diversi tipi di comportamento appena esaminati possono essere commessi direttamente dall'autore del reato. Tuttavia, è anche possibile utilizzare un bot per compiere questi atti. Questo ha il vantaggio che l'autore del reato deve impartire una sola volta le istruzioni al programma, che poi ripete automaticamente le azioni richieste tutte le volte che è necessario. C'è da temere che lo sviluppo dell'intelligenza artificiale renderà questo lavoro ancora più semplice ed efficiente in futuro. Il WormGPT è senza dubbio il precursore di una nuova forma di violazione, in quanto consente di 15

implementare in altri sistemi informatici i contenuti generati dall'intelligenza artificiale,
che per il momento sono stati confinati in una sandbox informatica.

- 16 Detto questo, anche senza l'utilizzo di un bot, l'intelligenza artificiale offre già innumerevoli possibilità di modificare i dati. Ad esempio, è molto facile chiedere di riscrivere un testo sostituendo un'idea con un'altra, o di modificare un'immagine sostituendo un elemento con un altro. In futuro, quindi, sarà sempre più difficile distinguere i dati autentici da quelli modificati.
- 17 Nella stragrande maggioranza dei casi, le violazioni dei dati si realizzano commettendo una condotta punibile. Tuttavia, le violazioni dei dati possono verificarsi anche a causa di una protezione inadeguata del sistema informatico. A nostro avviso, in questi casi si può parlare di commissione per omissione da parte dell'amministratore del sistema informatico che, in virtù della sua funzione, ha il dovere legale di agire e si trova quindi nella posizione di garante nei confronti del titolare dei dati.

C. Illecito

- 18 Per essere punibile, l'autore deve aver agito senza diritto. È il legittimo proprietario dei dati a stabilire chi è autorizzato a modificarli. Chiunque non sia stato autorizzato a modificare i dati è pertanto perseguibile. Non sono invece perseguibili le persone che sono state autorizzate, espressamente o tramite accordo, a modificare i dati dall'avente diritto, o che sono autorizzate a farlo per legge o per contratto.
- 19 Oggigiorno è frequente che i dati vengano modificati con un atto conclusivo. È il caso, ad esempio, dello scambio di messaggi tramite instant messenger come WhatsApp, Telegraph o Threema. Tutte queste applicazioni criptano i dati prima di inviarli e li decriptano quando li ricevono. Si tratta di una modifica dei dati. Tuttavia, è lecita, in primo luogo perché è accettata dagli utenti con un atto vincolante e, in secondo luogo, perché garantisce la riservatezza dei dati.
- 20 Un altro caso di modifica dei dati con atto vincolante è rappresentato dagli aggiornamenti delle applicazioni. Durante un aggiornamento, viene installata una nuova versione del programma al posto di quella precedente. I dati esistenti vengono cancellati e i nuovi dati vengono scritti e registrati sul

supporto di memorizzazione. Questo processo è lecito, purché l'utente abbia la possibilità di scegliere se installare o meno l'aggiornamento. A nostro avviso, l'editore dell'applicazione che obbliga l'utente a installare una nuova versione dell'applicazione, pena l'inutilizzabilità della stessa o l'illeggibilità dei dati, è punibile.

Per quanto riguarda gli atti autorizzati dalla legge, alcune leggi nazionali 21 contengono eccezioni alla garanzia di integrità dei dati. In particolare, consentono alle autorità penali o ai servizi di intelligence di installare govware nei sistemi informatici al fine di monitorare l'attività delle persone che li utilizzano, ad esempio per scoprire l'autore di un reato o per ottenere informazioni utili alla protezione dello Stato. L'installazione di questi programmi di spionaggio non è illegale, a condizione che venga effettuata nel rigoroso quadro stabilito dalla legge. Tuttavia, la sorveglianza può essere effettuata solo in casi gravi e deve essere soggetta a un successivo controllo giudiziario.

Anche la modifica dei dati non è illegale se è stata autorizzata 22 contrattualmente. Ciò vale in particolare per l'amministratore del sistema informatico che è responsabile della manutenzione. Non è punibile se aggiorna i programmi installati nel sistema informatico. È invece punibile chi approfitta del proprio status per cancellare o modificare i dati di un utente senza la sua autorizzazione.

Allo stesso modo, uno specialista informatico incaricato di effettuare test di 23 intrusione su un sistema informatico non è punibile se modifica i dati per creare una falla nelle difese messe in atto per proteggere l'accesso al sistema informatico. È invece punibile l'hacker che agisce nello stesso modo senza autorizzazione.

D. Intenzione

Una violazione dell'integrità dei dati deve essere intenzionale. L'intenzione 24 deve riguardare tutti gli elementi oggettivi del reato. L'autore deve quindi essere consapevole di danneggiare indebitamente i dati e avere la volontà di farlo. È sufficiente un'eventuale frode.

IV. ELEMENTO COSTITUTIVO AGGIUNTIVO FACOLTATIVO

- 25 L'articolo 4 cpv. 2 CCC consente agli Stati contraenti di formulare una riserva e di perseguire solo i comportamenti che hanno causato un danno grave.
- 26 Il testo non definisce il concetto di "danno grave". La relazione esplicativa si limita ad affermare che ogni Stato è libero di interpretare tale concetto come desidera. Tuttavia, le Parti hanno optato per il concetto di "danno" piuttosto che per quello di "danno". È quindi chiaro che il danno non si limita al solo aspetto economico. Il danno può quindi corrispondere anche al tempo di lavoro necessario per recuperare o ricreare i dati, nonché alle conseguenze della scomparsa o dell'impossibilità di utilizzare i dati.
- 27 Le parti hanno inoltre specificato che il danno deve essere grave. Questo aggettivo, unito al concetto di danno, significa che deve essere di una certa entità. È quindi ipotizzabile che il danno debba rappresentare una somma di denaro consistente, un numero significativo di ore di lavoro o avere gravi conseguenze.
- 28 L'Azerbaijan, la Lituania, la Repubblica Slovacca, il Cile e gli Stati Uniti d'America si sono avvalsi della possibilità prevista dall'art. 4 § 2 CPC. L'Azerbaijan, la Lituania, la Repubblica Slovacca e gli Stati Uniti d'America hanno specificato che nel loro diritto interno il concetto di danno grave deve essere interpretato come se avesse causato un danno grave. Il Codice penale slovacco è stato successivamente modificato. Il § 247 è stato sostituito dal § 247b. Nella sua forma semplice, il verificarsi di un danno grave non è più richiesto (§ 247b par. 1). D'altra parte, il verificarsi di un danno grave è diventato una forma qualificata del reato (§ 247b par. 2 let. a). Il Cile, da parte sua, ha parlato di danno grave. Si può quindi notare che, anche se la formulazione della Convenzione consentiva un'interpretazione molto ampia, tutti gli Stati che si sono avvalsi della possibilità offerta dall'art. 4 § 2 CCC hanno limitato il concetto di danno al solo aspetto economico.
- 29 È interessante notare il modo originale in cui il diritto svizzero ha affrontato la questione del danno grave. Invece di limitare l'azione penale alla condotta che ha causato un danno grave, l'art. 144^{bis} cap. 1 par. 2 del Codice Penale prevede una forma qualificata di azione penale quando il danno causato dall'autore è considerevole.

V. CONFRONTO CON IL DIRITTO SVIZZERO

Nel diritto svizzero, l'interferenza dei dati (art. 4 CCC) ha il suo corrispettivo 30 nell'art. 144^{bis} cap. 1 CP. Tuttavia, gli interessi giuridici tutelati da queste due disposizioni non sono strettamente identici, poiché l'art. 4 CCC tutela l'integrità e il corretto funzionamento o utilizzo dei dati o dei programmi informatici memorizzati, mentre l'art. 144^{bis} cap. 1 del Codice penale tutela il diritto all'integrità dei dati. Tuttavia, sono molto simili e condividono lo stesso scopo.

Le condotte punibili ai sensi dell'articolo 4 CCC sono tutte coperte 31 dall'articolo 144^{bis} cpv. 1, del Codice penale. I concetti di "danneggiamento", "deterioramento" e "alterazione" di cui all'articolo 4 del Codice penale sono coperti dal termine "modifica", che include tutte le forme di trasformazione. Il concetto di "cancellazione" cui fa riferimento la Convenzione, ossia la distruzione definitiva dei dati, è identico nel diritto svizzero. Infine, la "cancellazione" dei dati di cui all'art. 4 CCC è coperta dal termine "messa fuori uso", che comprende tutte le forme di comportamento con cui si impedisce al legittimo proprietario di utilizzare correttamente i propri dati.

Infine, l'art. 144^{bis} cpv. 1 del Codice penale svizzero prevede un reato che può 32 essere perseguito solo a querela di parte. Tuttavia, quando un reato è perseguito solo sulla base di una denuncia, l'autorità penale non può assumere la giurisdizione in prima persona. Poiché vi sono pareri discordanti sul fatto che una denuncia presentata nello Stato richiedente sia sufficiente per attuare la cooperazione internazionale, sarebbe prudente perseguire il deterioramento dei dati d'ufficio in tutti i casi, oppure presentare una dichiarazione che limiti l'azione penale ai casi in cui il danno causato sia considerevole.

I concetti tecnici informatici contenuti in questo contributo sono stati redatti con l'aiuto di Yannick Jacquey, ICT Manager con diploma federale. Desideriamo ringraziarlo calorosamente per la sua assistenza.

BIBLIOGRAFIA

Corboz Bernard, Les infractions en droit suisse, vol. I, 3. éd., Berne 2010

Schmid Niklaus, Computer- sowie Check- und Kreditkartenkriminalität, Zurich 1994

Schwarzenegger Christian, Die internationale Harmonisierung des Computer- und Internetstrafrechts durch die Convention on Cybercrime, in : Strafrecht, Strafprozessrecht und Menschenrechte, Festschrift Trechsel, Zurich 2002

Trechsel Stefan / Cramer Dean, in : Trechsel Stefan / Pieth Mark (éditeurs), Schweizerisches Strafgesetzbuch, Praxiskommentar, 4. éd., Zürich, 2021

Weissenberg Philippe, in : Niggli Marcel Alexander / Wiprächtiger Hans (éditeurs), Basler Kommentar, Strafrecht II, 4. éd., Bâle 2018

I MATERIALI

Conseil de l'Europe, Explanatory Report to the Convention on Cybercrime, Budapest 23.11.2001, disponible à <https://rm.coe.int/16800cce5b>, visité le 21.1.2024 (cité : Rapport explicatif de la Convention sur la cybercriminalité)

ATTENZIONE: Questa versione del commentario è una traduzione automatica dell'originale. Il commentario originale è in francese. La traduzione è stata effettuata con www.deepl.com. Solo la versione originale fa fede. La forma tradotta del commentario non può essere citata

COMMENTO SU

Art. 5 CCC (Convenzione sulla cibercriminalità [Cybercrime Convention])

Un commentario di Jérémie Müller

CITAZIONE SUGGERITA

Jérémie Müller, Commentario all'art. 5 CCC, in: Damian K. Graf (a cura di), Commentario online alla Convenzione sulla cibercriminalità (Cybercrime Convention)

Breve citazione: OK-Müller, art. 5 CCC N. XXX.

Art. 5 Attacco all'integrità di un sistema

Le Parti adottano le misure legislative e di altra natura necessarie per definire come reato, nel loro diritto interno, l'ostacolare in modo serio, intenzionale e illecito il funzionamento di un sistema informatico inserendo, trasmettendo, danneggiando, cancellando, deteriorando, alterando o sopprimendo dati informatici.

STRUTTURA

I. Aspetti generali	69
II. Beni giuridicamente protetti	69
III. Elementi costitutivi di base	70
A. Un sistema informatico	70
B. Condotta punibile	70
1. L'introduzione di dati	70
2. Trasmissione di dati	71
3. Danneggiamento, deterioramento e alterazione dei dati	72
4. Eliminazione e cancellazione dei dati	73
5. Modalità di commissione	73
C. Grave interferenza con il funzionamento del sistema informatico	74
D. Illecito	75
E. Intenzione	76
IV. Confronto con il diritto svizzero	76
Bibliografia	78
I Materiali	78

I. ASPETTI GENERALI

Negli ultimi decenni la società ha subito profondi cambiamenti. Molti servizi 1
sono diventati digitali. Gli smartphone, che non esistevano nemmeno
vent'anni fa, sono ormai onnipresenti nella vita di tutti. Consapevoli di questo
cambiamento, le aziende hanno adattato i loro servizi a questi nuovi
dispositivi e la maggior parte di esse offre servizi online. Questa tendenza di
fondo è stata ulteriormente accelerata dalla pandemia di coronavirus che ha
colpito la popolazione mondiale tra il 2020 e il 2022. Le misure sanitarie
messe in atto dalle autorità hanno limitato notevolmente i contatti tra gli
individui. Di conseguenza, il commercio ha dovuto trovare nuovi modi di fare
affari per sopravvivere.

Oggi, più che mai nella storia dell'umanità, tutti gli attori della società sono 2
interconnessi. Con i loro smartphone, le persone possono accedere ai loro
conti di e-banking, fare affari online, archiviare dati nel cloud o guardare
video in streaming da qualsiasi parte del mondo e in qualsiasi momento.

Tuttavia, questa estrema interconnessione crea un livello altrettanto elevato di 3
interdipendenza. Questa realtà è perfettamente illustrata dall'attacco
informatico su larga scala che ha colpito l'Estonia per diversi giorni nel 2007.
Uno dei Paesi più connessi al mondo è stato completamente paralizzato.
L'amministrazione statale, il sistema bancario, il commercio: nulla funzionava,
causando danni considerevoli alla società nel suo complesso. Oggi, ancor più
che nei primi anni 2000, è fondamentale che i sistemi informatici possano
funzionare senza intoppi.

In considerazione dei notevoli danni che possono derivare dall'ostacolare il 4
corretto funzionamento dei sistemi informatici, era indispensabile tutelare il
corretto funzionamento di questi sistemi con una norma penale.

II. BENI GIURIDICAMENTE PROTETTI

Il bene giuridico tutelato dall'articolo 5 CCC è il diritto del gestore e degli 5
utenti di un sistema informatico o di telecomunicazione di garantirne il
corretto funzionamento.

III. ELEMENTI COSTITUTIVI DI BASE

A. Un sistema informatico

- 6 Ai sensi dell'art. 1 let. a CCC, "l'espressione 'sistema informatico' indica qualsiasi dispositivo isolato o insieme di dispositivi interconnessi o collegati che, o uno o più elementi dei quali, effettuano un'elaborazione automatica di dati in esecuzione di un programma". Il concetto di sistema informatico comprende quindi tutti gli elementi hardware (scheda madre, processore, disco rigido, schermo, tastiera, stampante, ecc.) e software (BIOS, sistema operativo, software, aggiornamenti, ecc.), nonché i dispositivi che collegano tra loro questi diversi elementi (cavi, router, terminale wifi, ecc.).
- 7 Per maggiori dettagli su questo concetto, si rimanda a quanto scritto nel precedente art. 1 CCC.

B. Condotta punibile

- 8 L'articolo 5 del Codice penale elenca sette condotte punibili: inserire, trasmettere, danneggiare, cancellare, deteriorare, alterare o cancellare dati informatici. L'elenco è esaustivo. I comportamenti che interferiscono con il corretto funzionamento del sistema informatico, ma che non sono inclusi in questo elenco, non sono pertanto punibili. È il caso, ad esempio, dello spostamento di dati all'interno del sistema informatico, che è altrettanto dannoso del danneggiamento o del deterioramento dei dati.

1. L'introduzione di dati

- 9 Il concetto di introduzione deve essere interpretato nel senso che l'autore introduce nel sistema dati provenienti dall'esterno del sistema informatico di destinazione. Alcuni autori arrivano addirittura a camuffare questi dati facendoli apparire come file del tutto innocui, per evitare che vengano individuati troppo facilmente. Dall'esterno, questi dati appaiono quindi come dati originali del sistema.
- 10 Tuttavia, l'art. 5 CCC non si estende a tutti i dati immessi nel sistema informatico, ma solo a quelli destinati a interferire con il suo corretto funzionamento. Si tratta di dati o programmi dannosi che rallentano o addirittura bloccano completamente il funzionamento del sistema informatico. Questo risultato può essere ottenuto sia attivando una funzione

che rallenta o blocca il processo di elaborazione dei dati, sia disattivando una funzione necessaria al corretto funzionamento del sistema informatico. Tra gli esempi vi è l'installazione di un cavallo di Troia che consente all'autore di prendere il controllo di tutto o parte del sistema informatico, oppure l'installazione di un virus che paralizza il processore o distrugge un settore di avvio, impedendo al computer di riavviarsi.

2. Trasmissione di dati

Il termine "trasmissione di dati" si riferisce all'invio di dati da un sistema informatico a un altro. La condotta a cui si fa riferimento è l'invio di dati che interferiscono con il corretto funzionamento del sistema informatico. In particolare, le Parti hanno voluto criminalizzare gli attacchi di tipo denial of service e distributed denial of service. Un attacco di negazione del servizio consiste nell'invio di una tale quantità di dati a un sistema informatico bersaglio che quest'ultimo non è in grado di elaborare tutti i dati e finisce per bloccarsi. 11

Nel corso del tempo, le prestazioni dei sistemi informatici, in particolare dei server, sono aumentate notevolmente. Le tecniche di bilanciamento del carico e di alta disponibilità hanno reso gli attacchi di tipo denial of service quasi impossibili da realizzare. I criminali informatici hanno quindi trasformato l'attacco denial of service in un attacco denial of service distribuito. Questo attacco è simile al precedente, tranne per il fatto che l'autore ha il controllo di un gran numero di sistemi informatici, ai quali dà l'ordine di inviare simultaneamente grandi quantità di dati al sistema informatico bersaglio. Dato l'enorme volume di dati in arrivo da tutte le direzioni, il sistema informatico bersaglio non è in grado di elaborare tutti i dati e alla fine si blocca. Questo tipo di attacco è attualmente relativamente diffuso. È quasi sempre legato a richieste di riscatto in cambio dell'interruzione dell'attacco o a qualche altra frode come il furto di dati. Ancora oggi non esiste una soluzione per difendersi efficacemente dagli attacchi distributed denial of service. Inoltre, il danno causato alle vittime è particolarmente significativo, in quanto vengono private dell'uso del loro sistema informatico o impoverite dal pagamento del riscatto. 12

3. Danneggiamento, deterioramento e alterazione dei dati

- 13 L'integrità dei dati è essenziale per il corretto funzionamento dei sistemi informatici. La sua importanza è tale che è persino oggetto di uno standard ISO.
- 14 Il concetto di integrità dei dati si riferisce all'affidabilità, all'accuratezza e alla completezza dei dati. I dati di cui è garantita l'integrità sono quelli che non sono stati modificati dopo la loro registrazione iniziale. A titolo esemplificativo, il concetto di integrità garantita dei dati potrebbe essere paragonato all'invio di un pacco per posta, dove si certifica che il pacco è stato realmente spedito dal mittente indicato sul pacco, che tale invio è avvenuto nella data e nel luogo indicati dal timbro postale, che il pacco non è stato aperto durante il viaggio e che il contenuto del pacco non è stato alterato dopo l'invio.
- 15 Va da sé che il contenuto dei dati, ossia le informazioni in essi contenute (ad esempio testo, codice, immagine, ecc.), è altrettanto importante dell'integrità formale dei dati. Oltre a garantire l'integrità formale dei dati, è quindi essenziale garantire anche che il contenuto dei dati non sia stato corrotto. Nell'esempio del pacchetto riportato sopra, l'integrità formale dei dati è rappresentata dall'imballaggio, mentre l'integrità del contenuto dei dati corrisponde all'oggetto contenuto nel pacchetto.
- 16 Il danneggiamento e il deterioramento dei dati di cui all'art. 5 CCC sono comportamenti che si sovrappongono nel campo dell'informatica. In entrambi i casi, l'integrità o il contenuto dei dati o dei programmi viene compromesso. I dati danneggiati o deteriorati non sono più affidabili, accurati o completi. L'autore del reato modifica i dati del sistema informatico bersaglio in modo che non possano più essere utilizzati correttamente per l'elaborazione dei dati. Ad esempio, è sufficiente rinominare una cartella contenente file essenziali per il corretto funzionamento del sistema operativo per bloccare l'intero sistema informatico. Anche la modifica del codice di programmazione di un software può bloccare il corretto funzionamento. Più recentemente, i criminali informatici criptano i dati e poi vendono la chiave di crittografia.
- 17 L'alterazione si riferisce alla modifica dei dati esistenti nel sistema informatico, come conseguenza di un altro atto compiuto dall'autore del reato. Si tratta di un termine generico molto ampio che comprende tutte le modifiche apportate ai dati, ossia l'aggiunta, la sostituzione o la cancellazione

di dati. Queste modifiche possono riguardare sia l'integrità formale che il contenuto dei dati. È il caso, in particolare, dei dati modificati in seguito all'introduzione di un cavallo di Troia o all'installazione di un virus.

4. Eliminazione e cancellazione dei dati

I dati informatici vengono salvati su supporti di registrazione (ad esempio, 18 disco rigido, DVD, chiavetta USB, ecc.) nell'ordine in cui sono stati creati. Per poter recuperare i dati specifici quando l'utente ne ha bisogno, il sistema informatico stabilisce una sorta di indice per sapere dove si trovano i dati sul supporto.

L'eliminazione dei dati comporta la distruzione di tutto o parte di questo 19 indice, che permette di trovare la posizione dei dati. I dati esistono ancora, ma il sistema informatico non può più sapere dove si trovano sul supporto e quindi non può più accedervi.

A differenza della cancellazione, la cancellazione dei dati è la distruzione 20 definitiva dei dati. I dati non esistono più sul supporto di memorizzazione.

Quando l'autore cancella o cancella dati essenziali per il corretto 21 funzionamento del sistema informatico, come i dati che costituiscono il sistema operativo, il sistema diventa inutilizzabile e cessa di funzionare.

5. Modalità di commissione

I vari tipi di condotta appena esaminati possono ovviamente essere commessi 22 direttamente da una persona fisica. Tuttavia, ciò richiederebbe molto tempo. In pratica, quindi, i criminali informatici tendono a utilizzare malware o bot per compiere questi atti in modo automatico. Il rapidissimo sviluppo dell'intelligenza artificiale renderà sicuramente molto più semplice questo tipo di azione. Il WormGPT ci dà già un assaggio delle possibilità offerte dall'intelligenza artificiale, poiché consente di implementare in altri sistemi informatici contenuti generati dall'intelligenza artificiale, finora confinati in una sandbox informatica.

C'è anche la questione della commissione per omissione. Nella maggior parte 23 dei casi, la condotta punibile è commessa da criminali informatici che cercano di ostacolare il buon funzionamento del sistema informatico per ottenere qualcosa in cambio. Tuttavia, è anche ipotizzabile che il sistema informatico finisca per non funzionare più correttamente perché l'amministratore non si

preoccupa di effettuare gli aggiornamenti necessari. A nostro avviso, l'amministratore del sistema informatico è punibile in questo caso perché, in virtù della sua posizione, ha un dovere legale di agire e si trova quindi in una posizione di garanzia nei confronti del titolare del diritto e degli utenti del sistema informatico.

- 24 A nostro avviso, la soluzione è identica nel caso dell'amministratore del sistema informatico che non installa un firewall e/o un antivirus per proteggerlo e lascia quindi innumerevoli possibilità di attacco a terzi.

C. Grave interferenza con il funzionamento del sistema informatico

- 25 Per essere colpevoli di interferenza nel sistema, non è sufficiente che l'autore del reato attacchi l'integrità dei dati contenuti nel sistema informatico, poiché ciò costituirebbe un'interferenza nei dati ai sensi dell'art. 4 del Codice Civile. L'atto deve interferire seriamente con il funzionamento del sistema informatico.
- 26 La compromissione si verifica quando il sistema informatico non funziona più in modo ottimale. La formulazione dell'art. 5 del Codice civile è sufficientemente neutra da proteggere più funzioni. È quindi irrilevante quali funzioni siano compromesse. È altresì irrilevante che l'intero sistema informatico sia danneggiato o che lo siano solo alcune funzioni.
- 27 Il sistema informatico è danneggiato quando viene messo fuori uso. È compromesso anche quando un'applicazione non può più essere utilizzata. Ciò può accadere perché il codice informatico del programma è stato danneggiato o distrutto, oppure perché i dati che l'utente aveva salvato sono stati cancellati, eliminati o criptati. Anche il sistema informatico può essere compromesso a causa della riduzione delle prestazioni. Ciò accade, ad esempio, quando un criminale informatico prende il controllo remoto di un sistema informatico e lo utilizza come macchina zombie all'insaputa del proprietario. In questo modo, utilizza parte delle prestazioni del sistema informatico senza il consenso del legittimo proprietario, di solito per scopi malevoli. Infine, il buon funzionamento di un sistema informatico può essere compromesso da richieste eccessive. È il caso degli attacchi di tipo denial of service o distributed denial of service. Di per sé, il sistema informatico funziona normalmente, ma viene bombardato da così tante richieste

simultanee che non riesce a elaborarle abbastanza rapidamente e finisce per bloccarsi.

In base alla formulazione dello standard, l'ostruzione deve derivare da una condotta punibile. Dato che l'elenco dell'art. 5 CCC è esaustivo, per essere punibile l'ostruzione deve necessariamente derivare da una delle forme di condotta elencate. L'ostruzione derivante da altri comportamenti, come lo spostamento di dati all'interno del sistema informatico, non è punibile. 28

Per quanto riguarda il qualificatore "grave", questo non è stato deliberatamente definito per consentire a ciascuno Stato di definirlo liberamente. Per alcuni, l'impedimento grave può riferirsi al danno minimo causato dall'impedimento. Per altri, invece, si tratterà della portata dell'impedimento, come il blocco di qualsiasi connessione all'esterno di un sistema informatico. Gli autori della bozza "considerano 'grave' l'invio a un sistema informatico di dati la cui forma, volume o frequenza pregiudichi in modo significativo la capacità del proprietario o dell'operatore di utilizzare il sistema in questione o di comunicare con altri sistemi (è il caso dei programmi che minano i sistemi sotto forma di 'denial of service', codici maligni, come i virus, che impediscono o rallentano in modo significativo il funzionamento del sistema, o programmi che inviano un'enorme quantità di posta elettronica a un destinatario al fine di paralizzare le funzioni di comunicazione del sistema)". 29

D. Illecito

Per essere punibile, l'autore deve aver agito senza diritto. È il legittimo proprietario del sistema informatico a stabilire chi ha il diritto di amministrare e utilizzare il sistema informatico. Ciò significa che chiunque non sia stato autorizzato a modificare il funzionamento del sistema informatico è perseguibile penalmente. D'altra parte, le persone che sono state autorizzate, espressamente o per atto notarile, dal legittimo proprietario a modificare il funzionamento del sistema informatico, così come coloro che sono autorizzati a farlo per legge o per contratto, non sono punibili. 30

Fino ai primi anni 2000, era raro che il sistema operativo o un'applicazione richiedessero un aggiornamento. Negli ultimi due decenni, tuttavia, gli aggiornamenti sono diventati sempre più comuni. Oggi sono addirittura la regola. Durante un aggiornamento, viene installata una nuova versione del 31

programma al posto di quella precedente. I dati esistenti vengono cancellati e i nuovi dati vengono scritti e registrati sul supporto di memorizzazione. Nella maggior parte dei casi, gli aggiornamenti contengono correzioni all'applicazione, correzioni di bug o nuove funzioni. A priori, quindi, non vi è alcuna forma di ostacolo al buon funzionamento del sistema informatico. Tuttavia, alcuni aggiornamenti possono richiedere più spazio sul disco rigido o occupare più RAM o capacità del processore. Questo rallenta il sistema informatico. Di conseguenza, il sistema informatico è rallentato e la sua capacità di funzionare correttamente è ostacolata. Nella maggior parte dei casi, questo non causa alcun problema, poiché il rallentamento del sistema informatico è molto lieve, se non addirittura insignificante. In casi eccezionali, gli aggiornamenti possono bloccare il funzionamento del sistema informatico, in particolare perché la versione precedente dell'applicazione utilizzava già il massimo delle risorse disponibili e l'aggiornamento richiede più risorse di quelle disponibili. In ogni caso, l'utente deve poter scegliere se installare o meno l'aggiornamento. A nostro avviso, l'editore dell'applicazione è punibile se costringe l'utente a installare una nuova versione dell'applicazione, senza la quale il sistema informatico non può funzionare correttamente o l'applicazione è resa inutilizzabile.

- 32 Le condotte elencate nell'art. 5 CCC non sono illecite anche quando sono state autorizzate contrattualmente. Ciò vale in particolare per l'amministratore del sistema informatico, il cui compito è la manutenzione del sistema. Non è punibile se aggiorna i programmi installati nel sistema informatico. È invece punibile chi approfitta del proprio status per compromettere il corretto funzionamento del sistema informatico, ad esempio disinstallando programmi o cancellando dati.

E. Intenzione

- 33 Un attacco all'integrità del sistema deve essere intenzionale. L'intento deve riguardare tutti gli elementi oggettivi del reato. L'autore deve quindi avere la consapevolezza e l'intenzione di interrompere il corretto funzionamento di un sistema informatico senza essere autorizzato a farlo.

IV. CONFRONTO CON IL DIRITTO SVIZZERO

- 34 Nel diritto svizzero non esiste un equivalente dell'art. 5 CCC. Le varie forme di condotta potrebbero certamente dare l'impressione di un'analogia con il

deterioramento dei dati (art. 144^{bis} cpv. 1 del Codice penale svizzero). Tuttavia, questo non è il caso per tre motivi.

In primo luogo, i beni giuridicamente protetti dall'art. 5 CCC e dall'art. 144^{bis}, 35
cpv. 1, del Codice penale sono completamente diversi. Come spiegato in precedenza, l'articolo 5 CCC tutela l'interesse del gestore e degli utenti di un sistema informatico o di telecomunicazione a garantirne il corretto funzionamento, mentre l'articolo 144^{bis}, cpv. 1, del Codice Penale garantisce il diritto di disporre dei dati. In altre parole, il primo garantisce il corretto funzionamento di un mezzo di elaborazione dei dati, mentre il secondo tutela uno specifico diritto reale.

Poiché i beni giuridicamente protetti non sono gli stessi, anche le persone 36
danneggiate dai due reati non sono le stesse. La persona danneggiata dal danneggiamento dei dati (articolo 144^{bis}, paragrafo 1, del Codice penale) è il proprietario dei dati danneggiati. D'altra parte, il danno all'integrità del sistema (art. 5 CCC) colpisce la persona che ha diritto al sistema informatico.

Inoltre, sebbene questi due reati abbiano molti punti in comune, non possono 37
essere equiparati. L'interferenza nel sistema (art. 5 CCC) deve essere vista per certi versi come una forma speciale di corruzione di dati (art. 144^{bis}, cpv. 1 PC), poiché richiede che l'interferenza nei dati provochi un grave impedimento al funzionamento del sistema informatico. Si tratta di un elemento costitutivo aggiuntivo che non è richiesto dalla legge svizzera.

Infine, alcuni comportamenti rientrano nell'ambito di applicazione dell'art. 5 38
CCC anche se non sono punibili ai sensi dell'art. 144^{bis} cap. 1 PC. È il caso, ad esempio, dell'invio di "dati a un sistema informatico la cui forma, volume o frequenza compromette in modo significativo la capacità del proprietario o dell'operatore di utilizzare il sistema in questione o di comunicare con altri sistemi". Questi atti non sono inoltre adeguatamente puniti dall'art. 179^{septies} del Codice penale (uso improprio di apparecchiature di telecomunicazione) per tre motivi. In primo luogo, perché l'art. 179^{septies} del Codice Penale richiede uno scopo speciale - vale a dire il dolo o la malizia - oltre all'intenzione, cosa che non avviene con l'art. 5 del CCC. In secondo luogo, perché l'uso improprio di un impianto di telecomunicazione è solo una contravvenzione ed è quindi punibile solo con una multa. Tuttavia, l'articolo 13 § 1 del Codice penale stabilisce espressamente che i reati punibili ai sensi degli articoli da 2 a 11 del Codice penale devono essere puniti con pene anche

detentive. In terzo luogo, perché il favoreggiamento e il tentativo di minare l'integrità del sistema sono punibili ai sensi dell'art. 11 CPC, mentre il favoreggiamento e il tentativo di abuso di un impianto di telecomunicazione non sono punibili, in quanto costituiscono una contravvenzione (cfr. art. 105 cpv. 2 CP).

- 39 Alla luce di quanto precede, si deve concludere che la legge svizzera non è conforme all'articolo 5 del Codice penale. Pertanto, deve essere adattata.

I concetti tecnici informatici contenuti nel presente contributo sono stati redatti con l'aiuto del sig. Yannick Jacquey, ICT Manager con diploma federale. Desideriamo ringraziarlo calorosamente per la sua assistenza.

BIBLIOGRAFIA

Ottis Rain, Analysis of the 2007 Cyber Attacks against Estonia from the information warfare perspective, in : Proceedings of the 7th European Conference on information warfare and security, Plymouth, 2008, pp 163-168, disponibile a <https://ccdcoe.org/library/publications/analysis-of-the-2007-cyber-attacks-against-estonia-from-the-information-warfare-perspective/> visité le 02.11.2023

Schmid Niklaus, Computer- sowie Check- und Kreditkartenkriminalität, Zurich 1994

Trechsel Stefan/Cramer Dean, in : Trechsel Stefan/Pieth Mark (éditeurs), Schweizerisches Strafgesetzbuch, Praxiskommentar, 4. éd., Zurich 2021

Weissenberg Philippe, in : Niggli Marcel Alexander/Wiprächtiger Hans (éditeurs), Basler Kommentar, Strafrecht II, 4. éd., Bâle 2018

I MATERIALI

Conseil de l'Europe, Explanatory Report to the Convention on Cybercrime, Budapest 23.11.2001, disponibile a <https://rm.coe.int/16800cce5b>, visité le 21.01.2024 (cité : Rapport explicatif de la Convention sur la cibercriminalité)

ATTENZIONE: Questa versione del commentario è una traduzione automatica dell'originale. Il commentario originale è in francese. La traduzione è stata effettuata con www.deepl.com. Solo la versione originale fa fede. La forma tradotta del commentario non può essere citata

COMMENTO SU

Art. 6 CCC (Convenzione sulla cibercriminalità [Cybercrime Convention])

Un commentario di Jérémie Müller

CITAZIONE SUGGERITA

Jérémie Müller, Commentario all'art. 6 CCC, in: Damian K. Graf (a cura di), Commentario online alla Convenzione sulla cibercriminalità (Cybercrime Convention)

Breve citazione: OK-Müller, art. 6 CCC N. XXX.

Art. 6 Uso abusivo di dispositivi

¹ Le Parti adottano le misure legislative e di altra natura necessarie per definire come reato, nel loro diritto interno, se commessi intenzionalmente e illecitamente:

a. la produzione, la vendita, il procurare per l'uso, l'importazione, la distribuzione o la messa a disposizione in altro modo di:

i. dispositivi, inclusi programmi informatici, concepiti o predisposti principalmente per commettere un reato di cui agli articoli 2–5,

ii. password di un computer, codici d'accesso o analoghe informazioni informatiche che permettono di accedere a tutto un sistema informatico o a una sua parte, con l'intento di commettere un reato di cui agli articoli 2–5; e

b. il possesso di un elemento di cui alla lettera a numero i o ii, con l'intento di commettere un reato di cui agli articoli 2–5. Le Parti possono prevedere, nel loro diritto interno, che soltanto il possesso di un certo numero di tali elementi dia luogo a responsabilità penale.

² Questo articolo non intende imporre una responsabilità penale laddove la produzione, la vendita, il procurare per l'uso, l'importazione, la distribuzione o la messa a disposizione in altro modo di cui al paragrafo 1 non abbiano lo scopo di commettere un reato di cui agli articoli 2–5, come nel caso del collaudo autorizzato o della protezione di un sistema informatico.

³ Le Parti possono riservarsi il diritto di non applicare il paragrafo 1, purché tale riserva non concerna la vendita, la distribuzione o la messa a disposizione

STRUTTURA

I. Aspetti generali	82
II. Proprietà giuridicamente protette	82
III. Elementi costitutivi di base	83
A. Oggetto illecito	83
1. Un dispositivo che consente di commettere un reato di cui agli articoli da 2 a 5 del Codice penale.	83
2. I dati che consentono l'accesso a un sistema informatico allo scopo di commettere uno dei reati di cui agli articoli da 2 a 5 del Codice penale.	84
B. Condotta punibile	84
1. Produzione, vendita, ottenimento per l'uso, importazione, distribuzione o altre forme di messa a disposizione.....	84
2. Possesso	86
C. Illegalità	86
D. Intenzione	86
E. Dolo speciale	87
IV. Riserve	87
A. Condotta punibile	87
B. Materiale illecito	88
V. Confronto con il diritto svizzero	89
Bibliografia	90
I Materiali	90

I. ASPETTI GENERALI

- 1 In linea di principio, la commissione dei reati punibili ai sensi degli articoli da 2 a 5 del Codice penale richiede l'uso di strumenti informatici. Tuttavia, non tutti i criminali informatici sono in grado di creare autonomamente tali strumenti. Cercano quindi di acquistarli da terzi. Nel corso del tempo, questa richiesta ha portato alla creazione di un vero e proprio mercato nero, in particolare sulla rete oscura. Al giorno d'oggi, quasi tutti possono acquistare malware di qualsiasi tipo, affittare reti di bot o persino commissionare ai criminali informatici l'esecuzione di compiti specifici. In considerazione del rischio che questo mercato nero rappresenta per tutti i sistemi informatici e i loro utenti legittimi, le Parti hanno deciso di imporre sanzioni penali per alcuni atti potenzialmente pericolosi a monte, prima che vengano commessi i reati di cui agli articoli da 2 a 5 del Codice penale. L'articolo 6 del CCC si basa sugli strumenti adottati dal Consiglio d'Europa (Convenzione europea sulla tutela giuridica dei servizi ad accesso condizionato o ad accesso condizionato - ETS n. 178) e dall'Unione europea (Direttiva 98/84/CE del Parlamento europeo e del Consiglio, del 20 novembre 1998, sulla tutela giuridica dei servizi ad accesso condizionato o ad accesso condizionato), nonché sulle disposizioni adottate in alcuni paesi in questo settore.

II. PROPRIETÀ GIURIDICAMENTE PROTETTE

- 2 Penalizzando tutte le forme di commercio o di possesso di materiale destinato alla commissione di uno dei reati puniti dagli articoli da 2 a 5 del Codice penale, le Parti rendono punibili gli atti preparatori alla commissione di tali reati. L'obiettivo è quindi quello di rafforzare la protezione dei beni giuridici tutelati dagli articoli da 2 a 5 del Codice penale, ovvero l'inviolabilità e il corretto funzionamento dei sistemi informatici, nonché l'integrità, la disponibilità e la riservatezza dei dati.

III. ELEMENTI COSTITUTIVI DI BASE

A. Oggetto illecito

1. Un dispositivo che consente di commettere un reato di cui agli articoli da 2 a 5 del Codice penale.

Il concetto di dispositivo non è definito né nel testo della Convenzione né nella relazione esplicativa. A nostro avviso, un dispositivo ai sensi dell'articolo 6 del Codice penale è un insieme di parti, elementi o dati destinati a svolgere una o più funzioni specifiche. Ciò è dimostrato dal fatto che le parti citano espressamente il programma per elaboratore come esempio di dispositivo. Come risulta evidente dall'aggiunta delle parole "incluso", il concetto è inteso in modo molto più ampio dei soli programmi per computer. Oltre a virus, worm, cavalli di Troia, bombe logiche e altro malware, che rientrano indiscutibilmente tra i programmi coperti da questa disposizione, vi sono anche dispositivi hardware come microfoni, telecamere e robot.

Tuttavia, l'ambito di applicazione della norma è limitato ai dispositivi progettati o adattati per commettere uno dei reati punibili ai sensi degli articoli da 2 a 5 del Codice penale. Si tratta di dispositivi o programmi progettati, ad esempio, per alterare o addirittura distruggere i dati, o per interferire con il funzionamento dei sistemi, come i programmi virus, o i programmi progettati o adattati per accedere ai sistemi informatici. I dispositivi che non consentono di compiere tali atti non rientrano nell'art. 6 § 1 let. a cap. 1 CCC. Lo stesso vale per i dispositivi che consentono di commettere un altro reato, in particolare uno di quelli punibili ai sensi degli articoli da 7 a 10 del Codice penale.

Durante la stesura della Convenzione, si è discusso a lungo se i dispositivi contemplati dovessero essere quelli progettati esclusivamente o specificamente per consentire la commissione di reati, il che escluderebbe i dispositivi a doppio uso, o se dovessero essere inclusi anche questi ultimi. Le Parti hanno infine concluso che l'azione penale non doveva essere limitata ai dispositivi progettati esclusivamente per commettere reati, in quanto ciò avrebbe ridotto notevolmente il numero di casi a cui applicare lo standard. Tuttavia, le Parti hanno anche escluso la possibilità di estendere lo standard a tutti i dispositivi, compresi quelli leciti, che potrebbero consentire di commettere reati in un modo o nell'altro, poiché la commissione del reato

sarebbe dipesa unicamente dall'intenzione dell'autore. È stata quindi adottata una soluzione intermedia.

- 6 L'articolo 6 para. 1, lettera a, punto 1, del Codice penale copre quindi i dispositivi principalmente progettati o adattati per consentire la commissione di uno dei reati punibili ai sensi degli articoli da 2 a 5 del Codice penale. Questa formulazione esclude i dispositivi a doppio uso, a meno che lo scopo principale non sia quello di commettere un reato.

2. I dati che consentono l'accesso a un sistema informatico allo scopo di commettere uno dei reati di cui agli articoli da 2 a 5 del Codice penale.

- 7 Al fine di coprire tutti i mezzi utilizzati dai criminali informatici per commettere uno dei reati punibili ai sensi degli articoli da 2 a 5 del Codice penale, le Parti hanno reso punibili anche gli atti volti a rendere disponibili password, codici di accesso e dati informatici simili che consentono l'accesso a tutto o a parte di un sistema informatico (articolo 6 § 1 let. a cap. 2 del Codice penale). L'obiettivo è quello di eliminare qualsiasi scappatoia. Questo approccio è perfettamente giustificato alla luce del gran numero di password e altri dati di accesso rubati e messi in vendita sulla rete oscura.

B. Condotta punibile

- 8 Le Parti hanno inteso punire tutte le forme di messa a disposizione di oggetti illeciti, nonché il loro possesso. Non è invece punibile la semplice fornitura di istruzioni - ad esempio sotto forma di testi o video - su come fabbricare oggetti illeciti.

1. Produzione, vendita, ottenimento per l'uso, importazione, distribuzione o altre forme di messa a disposizione

- 9 L'art. 6 § 1 lett. a CCC elenca una serie di atti punibili relativi al commercio. L'elenco è esaustivo. Tuttavia, al fine di garantire che nessuna condotta venga trascurata, si conclude con una clausola generale ("Auffangtatbestand").
- 10 Per "produzione" si intende la fabbricazione di materiale illecito in vista del suo utilizzo per la commissione di uno dei reati elencati negli articoli da 2 a 5 del Codice penale. Il termine "produzione" comprende tutte le fasi necessarie

alla realizzazione dell'oggetto. Comprende quindi la scrittura del codice malware - in linguaggio informatico - o la decrittazione di una password.

L'art. 6 § 1 lett. a CCC sanziona poi la "vendita". Questo termine si riferisce alla 11
consegna di un oggetto illecito di cui al presente paragrafo in cambio di una
somma di denaro. La valuta in cui viene pagata la somma è irrilevante. Può
anche essere pagata in criptovalute. Tuttavia, la rimessa deve essere costosa.
Non può essere una donazione.

"Ottenere per l'uso" implica un comportamento attivo da parte della persona 12
che cerca di ottenere materiale proibito. La persona deve aver contattato
qualcuno in possesso del materiale proibito e averlo acquisito gratuitamente o
in cambio di un pagamento. Non è importante il modo in cui il materiale
viene consegnato. Il trasferimento può quindi avvenire per via elettronica, per
posta o anche tramite consegna a mano. Ciò che è decisivo è se l'autore
ottiene il materiale illegale con lo scopo di utilizzarlo per commettere uno dei
reati punibili ai sensi degli articoli da 2 a 5 del Codice penale. Se lo scopo è
commettere un altro reato o semplicemente raccogliere questo tipo di
materiale, l'autore non è punibile.

La quarta condotta menzionata nell'elenco è l'"importazione". Questo termine 13
si riferisce all'atto di introdurre un oggetto illecito nel Paese che lo sanziona.
L'importazione di materiale proibito crea un rischio significativo che esso
venga successivamente trasmesso a terzi. Per ridurre questo rischio, è vietata
la semplice introduzione nel Paese, anche se l'importatore è solo un anello
della catena tra il produttore del materiale e l'utente finale.

L'articolo 6 cpv. 1 punisce anche la "diffusione". Si tratta della trasmissione di 14
materiale illegale a un numero indeterminato di persone che non ne hanno
necessariamente fatto richiesta. Il materiale può essere inviato con qualsiasi
mezzo, sia esso informatico, postale o a mano.

Per evitare lacune, l'elenco si conclude con "altre forme di fornitura". Questa 15
ipotesi permette di comprendere tutti i casi che non corrispondono
esattamente ai concetti sopra esaminati, ma che tuttavia consentono all'autore
di fornire oggetti illeciti a terzi. Questa espressione include, ad esempio, la
creazione o la compilazione di link ipertestuali che hanno lo scopo di
facilitare l'accesso a materiale illecito.

2. Possesso

- 16 L'art. 6 § 1 lett. b CCC punisce il possesso di uno qualsiasi degli oggetti sopra menzionati. Come per le condotte elencate nell'art. 6 § 1 let. a CCC, l'autore deve possedere il materiale proibito con l'intenzione di commettere uno dei reati punibili ai sensi degli artt. 2-5 CCC. Se l'autore possiede questo materiale con l'intenzione di commettere un altro reato o semplicemente a scopo di collezione, non è punibile.
- 17 Le Parti hanno tuttavia lasciato a ciascuno Stato un certo margine di manovra nel determinare se il possesso di un singolo oggetto sia sufficiente per commettere il reato o se sia necessario il possesso di una serie di oggetti. Va detto, tuttavia, che questa possibilità sembra essere stata introdotta soprattutto a favore degli Stati Uniti d'America, che sono stati l'unico Paese a farne uso. Tuttavia, non hanno specificato il numero minimo di elementi che devono essere posseduti per essere punibili. Si riferivano semplicemente al numero previsto dalla legge federale statunitense applicabile.

C. Illegalità

- 18 Il requisito secondo cui l'autore deve aver agito senza diritto consente alle Parti di creare eccezioni alla responsabilità penale. In particolare, ciò consente loro di escludere dall'ambito di applicazione dell'articolo 6 CCC le autorità giudiziarie che detengono legittimamente materiale illegale, sotto forma di sequestro, nell'ambito delle loro indagini.
- 19 L'art. 6 § 2 riserva espressamente l'ipotesi in cui l'autore non agisca senza diritto, vale a dire che la condotta elencata nell'art. 6 § 1 let. a cap. 1 CCC non è punibile se il suo scopo non è quello di commettere un reato punibile ai sensi degli artt. 2-5 CCC. Pertanto, ad esempio, i dispositivi di test (noti anche come "dispositivi di cracking") e i dispositivi di analisi di rete progettati dai professionisti per valutare l'affidabilità dei loro prodotti informatici o per verificare la sicurezza dei sistemi sono prodotti per scopi legittimi e i loro utenti sono quindi considerati agire "legittimamente".

D. Intenzione

- 20 L'abuso di dispositivi è intenzionale. L'intento deve riguardare tutti gli elementi oggettivi del reato. Se l'autore possiede o fornisce a terzi un normale programma informatico senza sospettare che possa essere utilizzato anche

per commettere uno dei reati puniti dagli articoli da 2 a 5 del Codice penale, non è punibile.

E. Dolo speciale

Oltre al dolo, l'autore deve aver agito allo scopo di commettere uno dei reati di cui agli articoli da 2 a 5 del Codice penale. Non è quindi sufficiente che l'autore voglia produrre un programma dannoso solo per la sfida tecnica che rappresenta o per raccoglierlo. Allo stesso modo, non è sufficiente che l'autore intenda utilizzare il programma dannoso o la password per commettere un reato diverso da quelli punibili ai sensi degli articoli da 2 a 5 del Codice penale. 21

Lo scopo perseguito dall'autore del reato deve essere la commissione, da parte sua o di un terzo a cui fornisce il materiale proibito, di uno dei reati punibili ai sensi degli articoli da 2 a 5 del Codice penale. L'articolo 6 del Codice penale stabilisce un reato di messa in pericolo astratto. Non è quindi necessario che il materiale illegale venga effettivamente utilizzato in seguito per commettere uno di questi reati. È sufficiente che l'atto punibile sia commesso allo scopo di commettere uno dei reati punibili ai sensi degli articoli da 2 a 5 del Codice penale. 22

IV. RISERVE

L'unica condotta che le Parti devono punire è la vendita, la distribuzione o qualsiasi altra fornitura di una password, di un codice di accesso o di dati informatici simili che consentano l'accesso a tutto o a parte di un sistema informatico. D'altra parte, esse possono limitare l'ambito di applicazione di questa norma in relazione ad altre condotte punibili e/o oggetti illeciti. 23

A. Condotta punibile

La Convenzione consente alle Parti di limitare l'azione penale rifiutando di perseguire la produzione, l'ottenimento per uso, l'importazione e il possesso di materiale illecito. 24

Georgia, Svizzera, Cile, Giappone e Sri Lanka si sono avvalsi di questa possibilità per limitare il più possibile le condotte punibili. 25

- 26 Il Principato di Andorra ha dichiarato che l'ottenimento per uso dei dispositivi di cui all'articolo 6(1)(a) CCC non è punibile ai sensi del suo diritto interno.
- 27 L'Azerbaijan ha dichiarato che avrebbe perseguito le condotte elencate all'articolo 6(1) CCC solo in caso di danni gravi.
- 28 L'Ucraina ha spiegato che non avrebbe punito l'ottenimento per uso e altre forme di messa a disposizione degli articoli di cui all'articolo 6 § 1 let. a n. 1 CCC, né la produzione e l'ottenimento per uso degli articoli di cui all'articolo 6 § 1 let. a n. 2 CCC.
- 29 Gli Stati Uniti d'America si sono riservati il diritto di non perseguire la produzione, l'approvvigionamento per l'uso, l'importazione e il possesso di materiale illecito progettato o adattato per consentire la commissione dei reati puniti dagli articoli 4 e 5 del Codice penale.
- 30 Israele ha dichiarato che non perseguirà l'ottenimento per l'uso o l'importazione di materiale illecito, o il possesso di una password, di un codice di accesso o di dati informatici simili che consentono l'accesso a tutto o a parte di un sistema informatico.
- 31 La Germania, il Principato di Andorra, l'Argentina e il Perù si sono limitati a rifiutare di perseguire il possesso di materiale illecito (art. 6 § 1 let. b CCC).

B. Materiale illecito

- 32 La Convenzione consente inoltre alle Parti di limitare l'azione penale rifiutando di considerare illeciti i dispositivi, compresi i programmi informatici, che sono principalmente progettati o adattati per consentire la commissione di uno dei reati punibili ai sensi degli articoli da 2 a 5 del Codice penale.
- 33 Anche Georgia, Norvegia, Svizzera, Giappone e Sri Lanka si sono avvalsi di questa possibilità per limitare il più possibile il materiale punibile.
- 34 Il Cile ha inizialmente formulato la stessa riserva di Georgia, Norvegia, Svizzera e Giappone. Tuttavia, ha modificato la propria legislazione nel 2022. Nella nuova versione, l'abuso di dispositivi corrisponde all'art. 6 CCC. La riserva non è quindi più necessaria.

Gli Stati Uniti si sono riservati il diritto di non perseguire i dispositivi, 35
compresi i programmi informatici, progettati o adattati per consentire la
commissione dei reati puniti dagli articoli 4 e 5 del Codice penale.

La Germania ha dichiarato che un dispositivo, compreso un programma per 36
computer, progettato o adattato principalmente per consentire la
commissione di un reato punibile ai sensi degli articoli da 2 a 5 del codice
civile non è materiale punibile ai sensi della legge tedesca.

V. CONFRONTO CON IL DIRITTO SVIZZERO

Nel suo messaggio relativo all'approvazione e all'attuazione della 37
Convenzione del Consiglio d'Europa sulla criminalità informatica, il Consiglio
federale ha affermato che l'art. 6 CCC è essenzialmente coperto dall'art. 144^{bis}
cpv. 2 del Codice penale e dall'aggiunta di un secondo cpv. all'art. 143^{bis} del
Codice penale.

Tuttavia, anche se la Svizzera ha sfruttato tutte le possibilità offerte dall'art. 38
6(3) CCC per limitare al massimo la condotta punibile e il materiale illecito,
resta il fatto che il diritto svizzero è ben lontano dal soddisfare i requisiti
minimi stabiliti dall'art. 6 CCC, per diverse ragioni.

In primo luogo, l'art. 144^{bis} c. 2 c. 1 del Codice penale si applica solo al 39
software. Non si applica quindi ad altri dispositivi, password, codici di accesso
o dati informatici simili. Inoltre, il software di cui all'art. 144^{bis} co. 2 co. 1 del
Codice Penale deve essere progettato o destinato a commettere un reato
punibile ai sensi dell'art. 144^{bis} co. 1 co. 1 del Codice Penale. Ciò solleva due
problemi. Da un lato, l'Art. 144^{bis} (1) (1) CP non soddisfa pienamente i requisiti
minimi dell'Art. 4 CCC. In secondo luogo, l'Art. 144^{bis} cpv. 2 (1) del Codice
Penale ignora completamente il software progettato o destinato a commettere
un reato corrispondente a quelli punibili ai sensi degli Art. 2, 3 o 5 del Codice
Penale. Tale software non è quindi punibile secondo la legge svizzera.

L'aggiunta dell'art. 143^{bis} cpv. 2 del Codice Penale svizzero colma solo una 40
piccola parte di queste importanti lacune. Infatti, questa disposizione punisce
solo l'atto di mettere in circolazione o rendere accessibile una password, un
programma o qualsiasi altro dato idoneo o destinato a commettere il reato
punito dall'art. 143^{bis} cpv. 1 del Codice Penale. Da un lato, questo standard
non soddisfa i requisiti minimi dell'art. 2 CCC. In secondo luogo, non rende
reato la distribuzione o la messa a disposizione di una password, di un

programma o di qualsiasi altro dato idoneo o destinato a essere utilizzato per la commissione di un reato diverso da quello punito dall'art. 143^{bis} cpv. 1 del Codice Penale.

- 41 In definitiva, anche supponendo che l'articolo 143^{bis} cpv. 1 del Codice Penale soddisfi i requisiti dell'articolo 2 del CCC e che l'articolo 144^{bis} para. 1 cpv. 1 del Codice Penale soddisfi i requisiti minimi dell'articolo 4 del CCC, la punibilità ai sensi della legge svizzera sarebbe limitata alla diffusione o alla messa a disposizione di una password, di un programma o di qualsiasi altro dato idoneo o destinato all'uso per la commissione del reato punito dall'articolo 2 del CCC, nonché alla messa a disposizione di una password, di un programma o di qualsiasi altro dato idoneo o destinato all'uso per la commissione del reato punito dall'articolo 4 del CCC. 2 CCC, nonché di fabbricare, importare, mettere in circolazione, promuovere, offrire o mettere a disposizione in altro modo un software idoneo o destinato a commettere il reato punito dall'art. 4 CCC.
- 42 Per soddisfare i requisiti minimi dell'art. 6 CCC, gli artt. 143 cpv. 1, 143^{bis} cpv. 1 e 144^{bis} n. 1 cpv. 1 del Codice Penale dovrebbero quindi essere modificati come descritto sopra; l'equivalente dell'art. 5 CCC e completare ciascuno di essi. 5 CCC e completare ciascuna di queste disposizioni aggiungendo un paragrafo che renda reato la vendita, la distribuzione o la messa a disposizione in altro modo di una password, di un codice di accesso o di dati informatici simili che consentano l'accesso a tutto o a parte di un sistema informatico, allo scopo di commettere uno di questi quattro reati.

BIBLIOGRAFIA

Trechsel Stefan/Cramer Dean, in : Trechsel Stefan/Pieth Mark (Hrsg.), Schweizerisches Strafgesetzbuch, Praxiskommentar, 4. éd., Zurich 2021

Weissenberg Philippe, in: Niggli Marcel Alexander/Wiprächtiger Hans (éditeurs), Basler Kommentar, Strafrecht II, 4. éd., Bâle 2018

I MATERIALI

Conseil de l'Europe, Explanatory Report to the Convention on Cybercrime, Budapest 23.11.2001, disponible à <https://rm.coe.int/16800cce5b>, visité le 21.1.2024 (cité : Rapport explicatif de la Convention sur la cybercriminalité)

Message relatif à l'approbation et à la mise en œuvre de la Convention du Conseil de l'Europe sur la cybercriminalité, FF 2010 4275, disponible à <https://www.fedlex.admin.ch/eli/fga/2010/813/fr>, visité le 21.1.2024

ATTENZIONE: Questa versione del commentario è una traduzione automatica dell'originale. Il commentario originale è in francese. La traduzione è stata effettuata con www.deepl.com. Solo la versione originale fa fede. La forma tradotta del commentario non può essere citata

COMMENTO SU

Art. 7 CCC (Convenzione sulla cibercriminalità [Cybercrime Convention])

Un commentario di Jérémie Müller

CITAZIONE SUGGERITA

Jérémie Müller, Commentario all'art. 7 CCC, in: Damian K. Graf (a cura di), Commentario online alla Convenzione sulla cibercriminalità [Cybercrime Convention]

Breve citazione: OK-Müller, art. 7 CCC N. XXX.

Titolo 2: Reati informatici

Art. 7 Falsificazione informatica

Le Parti adottano le misure legislative e di altra natura necessarie per definire come reato, nel loro diritto interno, se commessi intenzionalmente e illecitamente, l'inserimento, l'alterazione, la cancellazione o la soppressione di dati informatici da cui risultano dati non autentici, nell'intento di farli considerare o utilizzare a fini legali come se fossero autentici, indipendentemente dal fatto che siano direttamente leggibili o comprensibili. Le Parti possono prevedere che

soltanto la presenza di un intento fraudolento o altrettanto illegale dia luogo a responsabilità penale.

STRUTTURA

I. Aspetti generali	96
II. Beni giuridicamente protetti	96
III. Elementi costitutivi di base	96
A. Dati informatici	96
B. Dati rilevanti per i rapporti giuridici	97
C. Condotta punibile	98
1. Immissione di dati	99
2. Alterazione, eliminazione e cancellazione dei dati	99
D. Illegalità	100
E. Intenzione	100
IV. Elementi costitutivi aggiuntivi facoltativi	101
V. Confronto con il diritto svizzero	102
I Materiali	102

I. ASPETTI GENERALI

- 1 Data l'ubiquità delle tecnologie informatiche nella società, la falsificazione di documenti informatici è altrettanto pericolosa della falsificazione di documenti cartacei. Lo scopo di questa disposizione è quindi quello di introdurre un reato che sia la controparte della falsificazione di documenti cartacei. Essa intende colmare le lacune del diritto penale relative alla falsificazione tradizionale, che richiede la leggibilità visiva delle dichiarazioni contenute in un documento e non si applica ai dati registrati su un supporto elettronico. La manipolazione di dati registrati con valore probatorio può avere conseguenze altrettanto gravi della falsificazione tradizionale se induce in errore un terzo. La falsificazione informatica consiste nella creazione o nella modifica non autorizzata di dati registrati in modo tale da acquisire un valore probatorio diverso, cosicché la conduzione di operazioni legali, basate sull'autenticità delle informazioni fornite da tali dati, può essere inficiata dall'inganno.

II. BENI GIURIDICAMENTE PROTETTI

- 2 Il bene giuridico tutelato da questo standard è la sicurezza e l'affidabilità dei dati elettronici, che può avere conseguenze sui rapporti giuridici.

III. ELEMENTI COSTITUTIVI DI BASE

A. Dati informatici

- 3 Ai sensi dell'articolo 1, lettera b), del CDC, per "dati informatici" si intende qualsiasi rappresentazione di fatti, informazioni o concetti in una forma adatta all'elaborazione in un sistema informatico, compreso un programma progettato per far sì che un sistema informatico esegua una funzione. Il concetto di dati informatici è quindi molto ampio e comprende in particolare tutte le lettere, i simboli o i codici di programmazione che possono essere inseriti, elaborati e memorizzati da un sistema informatico.
- 4 Per maggiori dettagli su questo concetto, si rimanda a quanto scritto nel precedente art. 1 CCC.

B. Dati rilevanti per i rapporti giuridici

L'uso delle parole "per scopi legali" significa che l'art. 7 CCC non si applica a 5
tutti i dati informatici, ma solo ai dati che svolgono un ruolo nei rapporti
legali. Deve quindi essere possibile dimostrare un fatto di rilevanza giuridica,
ossia un fatto da cui dipende la creazione, la modifica o l'estinzione di un
diritto. Tutti i dati che non sono rilevanti per i rapporti giuridici sono quindi
esclusi dall'ambito di applicazione di questo standard.

Per essere probante, deve essere possibile stabilire l'origine dei dati. Nel 6
mondo reale, questo requisito significa che l'autore di un titolo deve essere
identificabile e che questo titolo contiene l'espressione di un pensiero umano.
In termini pratici, ciò significa, ad esempio, che le informazioni devono avere
un senso e che il documento deve essere firmato dal suo autore. Nel mondo
virtuale, la garanzia dell'origine dei dati assume una forma molto diversa.
Naturalmente, esiste l'equivalente di un documento cartaceo firmato dal suo
autore. Si tratta di un documento informatico redatto da un essere umano in
cui la firma autografa è sostituita da una firma elettronica qualificata. Tuttavia,
il mondo virtuale offre molte altre possibilità di produrre dati rilevanti per i
rapporti giuridici.

A differenza dei titoli emessi nel mondo reale, nel mondo virtuale l'autore dei 7
dati non deve essere necessariamente un essere umano. Alcuni dati possono
essere generati automaticamente da sistemi informatici senza perdere il loro
valore probatorio. Ne sono un esempio una ricevuta di pagamento creata da
un'applicazione di e-banking, un certificato di stipendio per il fisco generato
automaticamente dal sistema informatico di un'azienda per i suoi dipendenti
alla fine dell'anno, o una ricevuta inviata automaticamente da un'autorità che
certifica che un documento legale è stato depositato per via informatica.

Come espressamente indicato nell'articolo 7 del Codice civile, questa 8
disposizione si estende a tutti i dati rilevanti per i rapporti giuridici
"indipendentemente dal fatto che siano o meno direttamente leggibili e
intelligibili". Non è quindi essenziale che i dati contengano l'espressione di un
pensiero umano. I dati possono essere stati generati da un sistema
informatico. È sufficiente che siano comprensibili da un essere umano o da
una macchina. I dati possono quindi assumere la forma di una sequenza di
caratteri che formano un codice, un codice a barre o un codice QR. L'esempio
più recente di questo tipo di dati è il certificato COVID generato dal computer

sotto forma di codice QR, che certifica che una persona è stata vaccinata contro il COVID e consente al suo titolare di accedere a determinati luoghi.

- 9 In definitiva, nel mondo virtuale, affinché i dati abbiano valore probatorio e possano essere utilizzati nei rapporti giuridici, è sufficiente che la loro origine possa essere stabilita con certezza e che possano essere compresi da un essere umano o da una macchina.

C. Condotta punibile

- 10 La definizione di falsificazione di documenti varia notevolmente da un Paese all'altro. È sufficiente un semplice confronto con la definizione data in Svizzera e nei Paesi limitrofi. In alcuni Paesi, il concetto di falsificazione si basa sull'autenticità dell'autore del documento, mentre in altri è determinante la veridicità delle informazioni contenute nel documento. Le Parti hanno pertanto convenuto che la falsificazione debba riguardare almeno l'identità dell'emittente dei dati, indipendentemente dall'accuratezza o dalla veridicità del contenuto dei dati. Tuttavia, esse sono libere di estendere l'ambito di applicazione delle loro disposizioni nazionali anche alla falsificazione delle informazioni contenute nel documento.
- 11 L'autenticità dei dati per quanto riguarda il loro autore implica che essi provengano effettivamente dalla persona da cui sembrano provenire. In questo senso, la falsificazione di dati autentici consiste nel rivelare un autore che non è la persona da cui i dati provengono effettivamente. L'autore reale non è quindi lo stesso dell'autore apparente.
- 12 L'autenticità in termini di contenuto dei dati significa che i dati sono rimasti nel loro stato originale. La falsificazione si verifica quindi quando i dati sono stati modificati dopo la loro creazione. La modifica di cui all'art. 7 del Codice Civile non è la semplice correzione di un errore materiale, ma la modifica del significato dei dati.
- 13 L'articolo 7 del Codice penale elenca quattro atti punibili: inserire, alterare, cancellare o sopprimere dati informatici. L'elenco è esaustivo. L'introduzione di dati punisce la creazione di un documento falso, mentre l'alterazione, la cancellazione e la soppressione riguardano la falsificazione di un documento vero.

1. Immissione di dati

L'introduzione di dati è l'atto con cui l'autore introduce nel sistema dati 14
provenienti dall'esterno di un sistema informatico. Ciò può comportare
l'inserimento non autorizzato di dati precisi o l'aggiunta di dati inesatti.

L'articolo 7 CCC sanziona solo l'introduzione di dati che portano alla 15
creazione di dati non autentici. Se i dati introdotti nel sistema informatico
hanno lo scopo di ostacolarne il corretto funzionamento, si applica l'art. 5
CCC.

Un esempio di introduzione di dati non autentici potrebbe essere il contabile 16
di una società che registra nel programma di contabilità un pagamento da
parte di un debitore, anche se il debitore in questione non ha effettivamente
pagato. Un altro esempio potrebbe essere quello di una persona che utilizza
una carta bancaria che ha copiato in modo fraudolento per pagare i suoi
acquisti utilizzando la funzione contactless, facendo così credere al terminale
del venditore che il pagamento è stato autorizzato ed effettuato dal legittimo
titolare della carta copiata.

2. Alterazione, eliminazione e cancellazione dei dati

L'alterazione dei dati consiste nel danneggiarne l'integrità e/o il contenuto. 17
L'integrità dei dati si riferisce all'affidabilità, all'accuratezza e alla completezza
dei dati. Nel mondo reale, la garanzia dell'integrità dei dati potrebbe essere
paragonata a un pacco spedito per posta, dove si certifica che è stato
realmente spedito dal mittente indicato sul pacco, che è stato spedito nella
data e nel luogo indicati dal timbro postale e che il pacco non è stato aperto
durante il viaggio. Per quanto riguarda la garanzia del contenuto, questa
potrebbe essere paragonata alla certificazione che il contenuto del pacco non
è stato alterato dopo l'invio. Nel caso dell'alterazione dei dati, l'autore
modifica il contenuto del pacco e/o il suo imballaggio per ingannare il
destinatario. L'alterazione del contenuto dei dati comporta la sostituzione dei
dati originali con altri dati. Ciò avviene, ad esempio, quando l'autore altera un
testo, cambia i dati bancari o sostituisce un'immagine con un'altra. D'altro
canto, l'autore altera l'integrità dei dati quando modifica i metadati. È il caso,
ad esempio, di chi falsifica l'indirizzo e-mail del mittente per far credere che
un messaggio provenga da una certa persona, mentre in realtà proviene da

un'altra, o falsifica una firma elettronica qualificata per far credere che un documento sia stato redatto da una certa persona, mentre in realtà non è così.

- 18 La cancellazione dei dati consiste nell'occultare e nascondere i dati. L'autore del reato rimuove deliberatamente una parte dei dati, in modo che il destinatario non abbia accesso a tutti i dati. È il caso, ad esempio, dell'autore che cancella parte delle clausole negoziate durante i colloqui transazionali, allo scopo di concludere un contratto a lui più favorevole.
- 19 A differenza della cancellazione dei dati, la cancellazione dei dati è la distruzione definitiva di tutti o parte dei dati. I dati non esistono più. Tra gli esempi vi è quello di chi cancella parti di conversazioni elettroniche a lui sfavorevoli e poi produce la versione redatta come prova in un processo, o di chi cancella i dati contenuti in una cartella clinica computerizzata per nascondere un errore medico commesso.

D. Illegalità

- 20 L'autore deve agire senza diritto, cioè senza essere stato autorizzato dal legittimo proprietario. Per agire legittimamente, una persona deve ottenere il consenso dell'avente diritto al sistema informatico per inserire i dati o dell'avente diritto ai dati per modificarli.
- 21 Nella società odierna, molte aziende e autorità pubbliche lavorano con sistemi informatici. La maggior parte dei dipendenti di questi enti è autorizzata a inserire o modificare i dati. Tutte queste persone agiscono in modo lecito finché seguono le istruzioni che sono state loro impartite. Tuttavia, le loro azioni diventano illegali quando inseriscono o modificano dati in violazione delle istruzioni ricevute. È il caso, ad esempio, dell'addetto al registratore di cassa che ruba la merce e poi inserisce false vendite nel sistema informatico nel tentativo di cancellare le tracce del suo crimine.

E. Intenzione

- 22 La falsificazione informatica è intenzionale. L'intenzione deve riguardare tutti gli elementi oggettivi del reato. L'autore del reato deve quindi avere la consapevolezza e la volontà di creare dati falsi o di falsificare dati autentici con l'intenzione di utilizzarli nei rapporti giuridici.

IV. ELEMENTI COSTITUTIVI AGGIUNTIVI FACOLTATIVI

L'ultima frase dell'art. 7 CCC consente alle Parti di richiedere uno scopo speciale oltre al dolo. Questo scopo speciale può assumere la forma di un intento fraudolento o di un analogo intento pernicioso. La relazione esplicativa non fornisce alcuna indicazione su come debba essere inteso il concetto di intento fraudolento. A nostro avviso, l'intento fraudolento si riferisce all'intenzione dell'autore di ottenere un vantaggio indebito per sé o per un'altra persona. Questo vantaggio non deve necessariamente essere pecuniario. Può essere qualsiasi vantaggio che migliori la propria situazione personale o quella di altri. Tuttavia, il vantaggio ricercato deve essere indebito, cioè contrario alla legge. 23

Gli Stati Uniti d'America si sono avvalsi della possibilità offerta dall'art. 7 del CCC e hanno indicato che avrebbero perseguito la falsificazione informatica solo se commessa con intento fraudolento. 24

La Germania e il Perù hanno ripreso le due finalità menzionate nell'art. 7 del Codice civile, ossia che la falsificazione informatica deve essere commessa con intento fraudolento o con un intento criminale simile. 25

Il Belgio, da parte sua, ha dichiarato che avrebbe reso la falsificazione informatica un reato penale solo se commessa con intento fraudolento o doloso. 26

La Svizzera ha deciso di perseguire la falsificazione informatica solo se commessa con l'intenzione di procurare a se stessi o a terzi un vantaggio o di causare un danno. 27

Infine, il Cile aveva inizialmente spiegato che avrebbe perseguito la falsificazione informatica solo se fosse stata commessa con intento fraudolento e avesse causato danni a terzi. A nostro avviso, questa dichiarazione non è in linea con la formulazione dell'art. 7 CCC, in quanto una parte può solo richiedere un intento speciale aggiuntivo. Tuttavia, non è possibile richiedere che venga causato un danno, mentre l'art. 7 CCC punisce il reato di messa in pericolo. Nel 2022, tuttavia, il Cile ha modificato la propria legislazione. Nella nuova versione, la falsificazione informativa corrisponde all'art. 7 CCC. La riserva non è quindi più necessaria. 28

V. CONFRONTO CON IL DIRITTO SVIZZERO

- 29 L'art. 7 CCC mira a punire la falsificazione di documenti elettronici. Nel diritto svizzero, questo bene giuridico è tutelato dal reato di falsificazione di titoli (art. 251 CP), che dal 1° gennaio 1995 è stato esteso ai titoli informatici (art. 110 cpv. 4 CP).
- 30 La condotta punibile ai sensi dell'art. 7 CCC consiste nel falsificare dati con valore probatorio allo scopo di ingannare altri. L'introduzione di dati corrisponde alla creazione del documento falso. D'altra parte, l'alterazione, la cancellazione e la soppressione sono equivalenti alla falsificazione di un documento nel reato tradizionale di falsificazione di documenti.
- 31 La legge svizzera è quindi conforme ai requisiti dell'articolo 7 della Convenzione.

I MATERIALI

Conseil de l'Europe, Explanatory Report to the Convention on Cybercrime, Budapest 23.11.2001, disponible à <https://rm.coe.int/16800cce5b>, visité le 21.1.2024 (cité : Rapport explicatif de la Convention sur la cybercriminalité)

Message concernant la modification du code pénal suisse et du code pénal militaire (Infractions contre le patrimoine et faux dans les titres) ainsi que la modification de la loi fédérale sur l'approvisionnement économique du pays (Dispositions pénales) du 24 avril 1991, FF 1991 II 933, disponible à https://www.fedlex.admin.ch/eli/fga/1991/2_969_933_797/fr, visité le 21.1.2024

ATTENZIONE: Questa versione del commentario è una traduzione automatica dell'originale. Il commentario originale è in francese. La traduzione è stata effettuata con www.deepl.com. Solo la versione originale fa fede. La forma tradotta del commentario non può essere citata

COMMENTO SU

Art. 8 CCC (Convenzione sulla cibercriminalità [Cybercrime Convention])

Un commentario di Jérémie Müller

CITAZIONE SUGGERITA

Jérémie Müller, Commentario all'art. 8 CCC, in: Damian K. Graf (a cura di), Commentario online alla Convenzione sulla cibercriminalità [Cybercrime Convention]

Breve citazione: OK-Müller, art. 8 CCC N. XXX.

Art. 8 Frode informatica

Le Parti adottano le misure legislative e di altra natura necessarie per definire come reato, nel loro diritto interno, il cagionare intenzionalmente e illecitamente un danno patrimoniale a terzi:

- a. inserendo, alterando, cancellando o sopprimendo dati informatici;
- b. interferendo nel funzionamento di un sistema informatico;

con l'intento fraudolento o illegale di procurare, senza averne diritto, un beneficio economico a se stessi o a terzi.

STRUTTURA

I. Aspetti generali	106
II. Beni giuridicamente protetti	106
III. Elementi costitutivi di base	106
A. Un sistema informatico	106
B. Dati informatici	106
C. Condotta punibile	107
1. Manipolazione dei dati	107
a. Immissione di dati	107
b. Alterazione, eliminazione e cancellazione dei dati	107
2. Un attacco al funzionamento del sistema informatico	108
D. Danni alla proprietà	109
E. Illegalità	109
F. Intenzione	109
G. Un disegno speciale	110
IV. Confronto con il diritto svizzero	110
Bibliografia	111
I Materiali	112

I. ASPETTI GENERALI

- 1 Lo sviluppo delle tecnologie informatiche e la loro applicazione in tutti i settori, in particolare in quello dei trasferimenti di denaro, hanno trasformato questo settore in un vero e proprio paradiso per la criminalità economica. La facilità con cui si possono commettere i reati e la quasi totale assenza di rischio di azione penale hanno favorito il trasferimento dei reati economici "tradizionali" su Internet. Per contrastare questa forma di criminalità, l'art. 8 del Codice Penale prevede l'incriminazione di "qualsiasi manipolazione impropria durante il trattamento dei dati al fine di effettuare un trasferimento illecito di proprietà".

II. BENI GIURIDICAMENTE PROTETTI

- 2 Questa disposizione protegge i sistemi informatici da manipolazioni fraudolente effettuate allo scopo di arrecare danni a terzi e trarne profitto.

III. ELEMENTI COSTITUTIVI DI BASE

A. Un sistema informatico

- 3 Ai sensi dell'art. 1 let. a CCC, "l'espressione 'sistema informatico' indica qualsiasi dispositivo isolato o insieme di dispositivi interconnessi o collegati che, o uno o più elementi dei quali, effettuano un'elaborazione automatizzata di dati in esecuzione di un programma". Il concetto di sistema informatico comprende quindi tutti gli elementi hardware (scheda madre, processore, disco rigido, schermo, tastiera, stampante, ecc.) e software (BIOS, sistema operativo, software, aggiornamenti, ecc.), nonché i dispositivi che collegano tra loro questi diversi elementi (cavi, router, terminale wifi, ecc.).
- 4 Per maggiori dettagli su questo concetto, si rimanda a quanto scritto nel precedente art. 1 CCC.

B. Dati informatici

- 5 Ai sensi dell'art. 1 lett. b CCC, "per 'dati informatici' si intende qualsiasi rappresentazione di fatti, informazioni o concetti in una forma adatta all'elaborazione in un sistema informatico, compreso un programma destinato

a far eseguire una funzione a un sistema informatico". Il concetto di dati informatici è quindi molto ampio e comprende in particolare tutte le lettere, i simboli o i codici di programmazione che possono essere inseriti, elaborati e memorizzati da un sistema informatico.

Per maggiori dettagli su questo concetto, si rimanda a quanto scritto nel precedente art. 1 CCC.

C. Condotta punibile

L'art. 8 del Codice penale elenca una serie di atti punibili e li suddivide in due categorie. La prima riguarda la manipolazione dei dati, mentre la seconda si riferisce all'interferenza con il funzionamento del sistema informatico.

1. Manipolazione dei dati

a. Immissione di dati

L'inserimento di dati ha lo stesso significato di cui agli artt. 4, 5 e 7 CCC. Si riferisce quindi all'atto con cui l'autore del reato introduce dati dall'esterno di un sistema informatico. Tuttavia, l'art. 8 CCC non punisce l'introduzione di qualsiasi dato, ma solo di quelli che possono causare un danno economico.

In particolare, si ha introduzione di dati quando l'autore del reato, senza esserne autorizzato, inserisce una carta di debito in uno sportello automatico e digita il numero di identificazione personale per prelevare denaro, oppure quando l'autore del reato si collega a un portale di e-banking, al posto di un terzo, utilizzando un ID e una password che ha rubato e trasferisce indebitamente denaro.

b. Alterazione, eliminazione e cancellazione dei dati

Le nozioni di alterazione, cancellazione e cancellazione dei dati sono identiche a quelle degli articoli 4, 5 e 7 del Codice penale.

I dati sono alterati quando l'autore del reato ne pregiudica l'integrità, ossia l'affidabilità, l'accuratezza e la completezza. Ciò avviene, ad esempio, quando l'autore del reato modifica i metadati di un pagamento durante una transazione online, con il risultato che il sistema informatico della banca reindirizza i fondi verso un conto appartenente all'autore del reato anziché verso il conto del destinatario originario.

- 12 I dati vengono alterati anche quando l'autore del reato ne attacca il contenuto. Un esempio potrebbe essere quello in cui l'autore del reato modifica in background le coordinate bancarie o l'importo di un ordine di pagamento su una piattaforma di e-banking senza che l'utente se ne accorga, in modo che il pagamento risulti superiore al previsto e/o non venga accreditato sul conto previsto.
- 13 L'autore deve cancellare i dati se ostacola il libero accesso a tali dati. L'autore impedisce al sistema informatico di avere pieno accesso a tutti i dati a cui dovrebbe avere accesso. È il caso di un autore che, avendo un limite di credito con un'organizzazione di carte di credito, cancella i dati relativi a tale limite dal sistema informatico dell'organizzazione, per consentirgli di continuare a effettuare pagamenti di credito, pur sapendo che non avrà i mezzi per rimborsarli.
- 14 Infine, la cancellazione dei dati è la distruzione definitiva dei dati. Non esistono più. Si pensi all'autore che accede al sistema informatico del suo creditore e cancella tutti i dati relativi alla somma che deve, o alla persona che, nel corso di un'asta online, cancella le offerte più alte e le sostituisce con la propria offerta a un prezzo molto più basso.

2. Un attacco al funzionamento del sistema informatico

- 15 Per garantire che non venga trascurata alcuna condotta fraudolenta, l'art. 8 let. b CCC copre anche in generale "qualsiasi forma di interferenza con il funzionamento di un sistema informatico". Questa formulazione si riferisce ad atti quali la manomissione dell'hardware, le azioni che impediscono la stampa e gli atti che influenzano le registrazioni o i flussi di dati, nonché l'ordine di esecuzione dei programmi.
- 16 A differenza della condotta punibile ai sensi dell'articolo 5 del Codice penale, l'interferenza con il funzionamento del sistema informatico non deve essere necessariamente grave. Al contrario, deve essere finalizzata a causare un danno economico.
- 17 Un esempio potrebbe essere la manipolazione di un terminale di pagamento con carta bancaria per confermare un pagamento al venditore, quando in realtà il pagamento non è stato effettuato sul conto da addebitare.

D. Danni alla proprietà

La condotta sopra descritta è punibile solo se causa un danno economico a un'altra persona. Tale pregiudizio può essere economico o materiale; si tratta quindi di un concetto molto ampio che comprende sia i beni liquidi che le immobilizzazioni materiali o immateriali con un valore economico. Più in generale, può essere definito come qualsiasi lesione del patrimonio sotto forma di diminuzione delle attività, aumento delle passività, mancato aumento delle attività o mancata diminuzione delle passività. 18

Il testo dell'art. 8 CCC non stabilisce un importo minimo per la perdita finanziaria causata. Anche una perdita minima è sufficiente. 19

Non è nemmeno richiesto che la perdita sia definitiva. Può essere sufficiente una perdita temporanea o provvisoria. Una transazione bancaria fraudolenta che causa una perdita finanziaria al titolare del conto che è stato addebitato, ma che viene successivamente corretta quando la frode viene rivelata, costituisce un reato. 20

E. Illegalità

L'autore deve agire senza diritto, cioè senza essere stato autorizzato a farlo dal legittimo avente diritto, per legge o per contratto. 21

La persona a cui l'avente diritto affida il proprio login e la propria password per effettuare un pagamento con l'e-banking non agisce senza diritto, purché esegua rigorosamente le istruzioni ricevute. Se invece utilizza i propri diritti di accesso per aumentare l'importo del bonifico o modificare l'identità del beneficiario, agisce senza diritto. 22

L'amministratore di un portale di e-banking o di un negozio online, responsabile della sua manutenzione, non è perseguibile se modifica i dati o impedisce temporaneamente il funzionamento del sito web. Se invece approfitta del suo accesso, ad esempio per modificare i dati del conto di un cliente, è colpevole di frode informatica. 23

F. Intenzione

La frode informatica è intenzionale. L'intento deve riguardare tutti gli elementi costitutivi oggettivi, ossia sia la condotta punibile sia il verificarsi di una perdita finanziaria. 24

G. Un disegno speciale

- 25 Oltre al dolo, l'art. 8 CCC richiede che l'autore agisca in un disegno per procurare a sé o a terzi un vantaggio economico. A nostro avviso, il concetto di beneficio economico non deve essere inteso nel senso ristretto in cui viene utilizzato in contabilità. Al contrario, comprende tutti i vantaggi economici che portano a un arricchimento. In altre parole, si riferisce a qualsiasi miglioramento della situazione patrimoniale.
- 26 Ci riferiamo soprattutto a un aumento delle attività, a una diminuzione delle passività, a una non diminuzione delle attività o a un non aumento delle passività. In questi casi, l'arricchimento corrisponde, ad esempio, al prezzo dei beni consegnati ma non pagati, alla somma sottratta da un conto bancario o all'importo del servizio ottenuto a spese altrui.
- 27 A nostro avviso, il concetto di beneficio economico è ancora più ampio e si estende anche a qualsiasi vantaggio patrimoniale. È il caso dell'autore che può utilizzare una piattaforma di streaming a pagamento senza doverla pagare, di chi, al momento della prenotazione online, fornisce il numero di carta di credito di un terzo come garanzia per non dover sopportare il rischio di vedersi addebitare la carta di credito in caso di cancellazione tardiva, o di chi utilizza i dati di un terzo, come uno studente o un pensionato, per ottenere - a prezzo ridotto - servizi per i quali avrebbe dovuto pagare il prezzo pieno.
- 28 Il beneficio economico voluto dall'autore deve essere ottenuto gratuitamente. Se l'autore ha o ritiene di avere un diritto di proprietà corrispondente all'arricchimento ottenuto, non agisce senza diritto e non è quindi punibile. Allo stesso modo, non costituiscono frode informatica le attività commerciali concorrenti che possono causare un danno economico a una persona e un beneficio a un'altra, ma che non sono svolte con intento fraudolento o disonesto, come l'uso di programmi di raccolta di informazioni per competere su Internet.

IV. CONFRONTO CON IL DIRITTO SVIZZERO

- 29 Nel diritto svizzero, la disposizione che più si avvicina all'art. 8 CCC è l'art. 147 del Codice penale svizzero. Tuttavia, questa disposizione non soddisfa i requisiti dell'art. 8 CCC sotto diversi aspetti.

In primo luogo, i beni giuridici tutelati dalle due disposizioni sono diversi. 30
L'art. 8 CCC protegge i sistemi informatici da manipolazioni fraudolente con lo scopo di danneggiare la proprietà altrui e trarne profitto. L'articolo 147 del Codice penale svizzero, invece, protegge solo i beni, escludendo l'interesse del gestore di un sistema informatico a garantirne il corretto utilizzo.

Per quanto riguarda le condotte punibili, l'art. 147 del Codice penale svizzero 31 punisce l'uso scorretto, incompleto o improprio dei dati. Questi reati si sovrappongono in larga misura ai concetti di introduzione, alterazione, cancellazione o soppressione di dati informatici di cui all'art. 8 CCC. Tuttavia, l'articolo 147 del Codice penale lascia aperta un'importante lacuna, poiché non punisce la cancellazione di dati che avrebbero dovuto essere presenti nel sistema informatico.

Infine, l'art. 147 CP punisce solo la frode informatica causata dalla 32 manipolazione dei dati. La condotta di cui all'art. 8 let. b CCC non rientra quindi nell'ambito di applicazione dell'art. 147 CP. Questo punto è particolarmente problematico, poiché molti atti sfuggono alla punizione anche se la Svizzera si è impegnata a perseguirli.

Va detto che la legge svizzera non è conforme all'art. 8 CCC e dovrebbe 33 quindi essere adattata.

BIBLIOGRAFIA

Corboz Bernard, *Les infractions en droit suisse*, vol. I, 3. éd., Berne 2010

Fiolka Gerhard, in: Niggli Marcel Alexander/Wiprächtiger Hans (éditeurs), *Basler Kommentar, Strafrecht II*, 4. éd., Bâle 2018

Schmid Niklaus, *Computer- sowie Check- und Kreditkartenkriminalität*, Zurich 1994

Stratenwerth Günter/Bommer Felix, *Schweizerisches Strafrecht, Besonderer Teil I: Straftaten gegen Individualinteressen*, 8. éd., Berne, 2022

Trechsel Stefan/Cramer Dean, in : Trechsel Stefan/Pieth Mark (éditeurs), *Schweizerisches Strafgesetzbuch, Praxiskommentar*, 4. éd., Zurich 2021

I MATERIALI

Conseil de l'Europe, Explanatory Report to the Convention on Cybercrime, Budapest 23.11.2001, disponible à <https://rm.coe.int/16800cce5b>, visité le 21.1.2024 (cité : Rapport explicatif de la Convention sur la cybercriminalité)

ATTENZIONE: Questa versione del commentario è una traduzione automatica dell'originale. Il commentario originale è in francese. La traduzione è stata effettuata con www.deepl.com. Solo la versione originale fa fede. La forma tradotta del commentario non può essere citata

COMMENTO SU

Art. 9 CCC (Convenzione sulla cibercriminalità [Cybercrime Convention])

Un commentario di Jérémie Müller

CITAZIONE SUGGERITA

Jérémie Müller, Commentario all'art. 9 CCC, in: Damian K. Graf (a cura di), Commentario online alla Convenzione sulla cibercriminalità [Cybercrime Convention]

Breve citazione: OK-Müller, art. 9 CCC N. XXX.

Titolo 3: Reati concernenti il contenuto

Art. 9 Reati di pedopornografia

¹ Le Parti adottano le misure legislative e di altra natura necessarie per definire come reato, nel loro diritto interno, se commessi intenzionalmente e illecitamente:

a. la produzione di pedopornografia allo scopo di diffonderla attraverso un sistema informatico;

b. l'offerta o la messa a disposizione di pedopornografia attraverso un sistema informatico;

c. la diffusione o la trasmissione di pedopornografia attraverso un sistema informatico;

d. il procurare pedopornografia per se stessi o per terzi attraverso un sistema informatico;

e. il possesso di pedopornografia in un sistema informatico o un supporto di salvataggio di dati informatici.

² Ai fini del paragrafo 1, il termine «pedopornografia» include il materiale pornografico che raffigura:

a. un minore che adotta un comportamento sessuale esplicito;

b. un soggetto che sembra essere un minore che adotta un comportamento sessuale esplicito;

c. immagini realistiche raffiguranti un minore che adotta un comportamento sessuale esplicito.

³ Ai fini del paragrafo 2 il termine «minore» include tutte le persone di età inferiore ai 18 anni. Le Parti possono comunque prevedere un limite d'età inferiore, ma non meno di 16 anni.

⁴ Le Parti possono riservarsi il diritto di non applicare in tutto o in parte il paragrafo 1 lettere d ed e, e il paragrafo 2 lettere b e c.

STRUTTURA

I. Aspetti generali	116
II. Beni giuridicamente protetti	117
III. Elementi costitutivi di base	117
A. Una rappresentazione pedopornografica	117
1. Il mezzo della rappresentazione	117
2. Natura pornografica	117
3. La nozione di minore	118
4. Il concetto di pornografia infantile	119
B. Condotte punibili	119
C. Illegalità	122
D. Intenzione	122
IV. Riserve	123
A. Per quanto riguarda l'età dei minori raffigurati	123
B. Condotta punibile	124
C. Gli oggetti della rappresentazione	124
V. Confronto con il diritto svizzero	125
Bibliografia	125
I Materiali	126

I. ASPETTI GENERALI

- 1 L'avvento di Internet ha permesso gli scambi più remoti, rapidi ed efficienti che l'umanità abbia mai conosciuto. Tuttavia, ha anche fornito strumenti di comunicazione molto potenti a criminali che prima erano spesso isolati. È così che chi produce materiale pedopornografico ha potuto entrare in contatto con chi consuma questo tipo di materiale in tutto il mondo. Lo scambio di idee, fantasie e consigli tra pedofili ha contribuito a sostenere, incoraggiare o facilitare i reati sessuali contro i bambini.
- 2 Tuttavia, oltre a facilitare lo scambio di materiale pedopornografico, il mondo virtuale ha permesso di garantire un certo grado di anonimato agli autori e, di conseguenza, una forma di impunità. Non sorprende quindi che questo tipo di reato si sia sviluppato rapidamente con la diffusione di Internet.
- 3 L'art. 9 CCC risponde quindi alle preoccupazioni espresse dai membri del Consiglio d'Europa in occasione del secondo vertice del 1997 e riflette una tendenza internazionale a favore della messa al bando della pornografia infantile, come confermato dalla recente adozione del Protocollo opzionale alla Convenzione delle Nazioni Unite sui diritti del fanciullo sulla vendita di bambini, la prostituzione infantile e la pornografia infantile e dalla recente iniziativa della Commissione europea sulla lotta contro lo sfruttamento sessuale dei bambini e la pornografia infantile (COM2000/854).
- 4 Questa disposizione mira a rafforzare le misure di protezione per i bambini, in particolare contro lo sfruttamento sessuale, modernizzando il diritto penale in modo da limitare più efficacemente l'uso di sistemi informatici nella commissione di reati sessuali contro i bambini.
- 5 Negli anni successivi all'adozione della Convenzione sulla criminalità informatica, la pornografia infantile e, più in generale, lo sfruttamento sessuale dei bambini sono rimasti temi molto importanti. Ciò ha portato alla stesura della Convenzione del Consiglio d'Europa sulla protezione dei bambini contro lo sfruttamento e l'abuso sessuale, adottata a Lanzarote il 25 ottobre 2007. L'art. 20 di questo trattato si ispira in larga misura all'art. 9 del CCC.

II. BENI GIURIDICAMENTE PROTETTI

L'art. 9 CCC tutela due diversi beni giuridici. L'art. 9 § 2 let. a CCC protegge ⁶ direttamente l'integrità sessuale dei bambini. Per quanto riguarda l'art. 9 § 2 let. b e c CCC, esso tutela l'integrità sessuale dei minori in modo indiretto, vietando qualsiasi comportamento che, senza necessariamente causare danni al "bambino" rappresentato nel materiale in questione, potrebbe tuttavia incoraggiare o incitare i minori a partecipare a tali atti. Queste disposizioni fanno quindi parte di una sottocultura che sostiene l'abuso di minori.

III. ELEMENTI COSTITUTIVI DI BASE

A. Una rappresentazione pedopornografica

1. Il mezzo della rappresentazione

L'articolo 9 CCC - come l'articolo 20 della Convenzione del Consiglio ⁷ d'Europa sulla protezione dei minori contro lo sfruttamento e l'abuso sessuale - si riferisce esclusivamente alle rappresentazioni visive della pornografia infantile. Ciò include tutte le rappresentazioni che possono essere percepite con la vista, in particolare fotografie, disegni, schizzi, dipinti, incisioni, sculture, video e film. Le registrazioni audio e i testi non sono contemplati.

Ai sensi della Convenzione sulla criminalità informatica, la repressione è ⁸ limitata alle rappresentazioni visive in forma digitale. Il supporto su cui sono registrate è irrilevante. È quindi irrilevante che siano registrate su un disco rigido, una chiavetta USB, un DVD o persino nel cloud.

2. Natura pornografica

Il concetto di pornografia non è definito né nella Convenzione sulla ⁹ criminalità informatica né nella Relazione esplicativa. Il Rapporto esplicativo si limita ad affermare che tale concetto deve essere interpretato in base alle norme di diritto interno che riguardano la classificazione della rappresentazione come oscena, incompatibile con la morale pubblica o comunque avente un effetto perverso.

In Svizzera si considera pornografia tutto ciò che ha lo scopo di eccitare ¹⁰ sessualmente il consumatore, in cui la sessualità è talmente distaccata dalle sue componenti umane ed emotive che la persona è ridotta a puro oggetto

sessuale di cui si può disporre a piacimento. Il comportamento sessuale è rozzo ed eccessivamente enfatizzato. La pornografia comprende la rappresentazione insistente e ripetitiva di atti come la fellatio, il cunnilingus e la masturbazione. Questa definizione non sembra né licenziosa né particolarmente casta. Al contrario, sembra equilibrata e può quindi essere facilmente adottata a livello internazionale. Gli elementi cardine di questa definizione si ritrovano anche nell'articolo 20 della Convenzione del Consiglio d'Europa sulla protezione dei bambini contro lo sfruttamento e l'abuso sessuale - in gran parte ispirata all'articolo 9 del CCC - che al paragrafo 2 definisce la pornografia infantile come qualsiasi materiale che rappresenti visivamente un bambino impegnato in una condotta sessualmente esplicita, reale o simulata, o qualsiasi rappresentazione degli organi sessuali di un bambino a scopo prevalentemente sessuale. Questa definizione può quindi essere mantenuta.

- 11 Sebbene il testo dell'art. 9 CCC non lo menzioni espressamente, il materiale di interesse artistico, medico o scientifico non è considerato pornografico.
- 12 Determinare cosa sia artistico e cosa no è complicato, soprattutto nel contesto di una convenzione internazionale conclusa tra Stati con culture molto diverse. A nostro avviso, il carattere artistico dovrebbe essere valutato caso per caso. In generale, tuttavia, si può dire che un materiale può essere definito artistico quando l'artista presenta qualcosa in modo originale, intende trasmettere un messaggio ed è il risultato di una vera ricerca. Ciò è in contrasto con una rappresentazione grossolana, banale o volgare della realtà.
- 13 Per quanto riguarda il materiale medico o scientifico, esso è necessario per la formazione o la ricerca.

3. La nozione di minore

- 14 Sebbene le legislazioni nazionali di alcune Parti della Convenzione prevedano una maggiore età (ad esempio, Canada, Giappone e Stati Uniti d'America), le Parti hanno convenuto che il concetto di minore debba essere inteso, in linea di principio, come qualsiasi persona di età inferiore ai 18 anni (articolo 9, paragrafo 3, CCC). Come si vedrà nella successiva sezione IV, le Parti possono tuttavia formulare riserve per richiedere un limite di età inferiore. In ogni caso, tuttavia, tale limite deve essere di almeno 16 anni.

4. Il concetto di pornografia infantile

L'articolo 9 § 2 CCC definisce il concetto di pornografia infantile fornendo un 15
elenco di tre tipi di rappresentazioni punibili. L'elenco è esaustivo.

In primo luogo, vi sono le rappresentazioni di un minore che si impegna in 16
una condotta sessualmente esplicita. L'espressione "condotta sessualmente
esplicita" si riferisce soprattutto ai rapporti sessuali, compresi quelli genitali,
oro-genitali, ano-genitali o oro-anali. Per essere punibili ai sensi dell'art. 9 § 2
let. a CCC, devono coinvolgere almeno un minore. D'altra parte, è irrilevante
che avvengano solo tra minori o con uno o più adulti. Anche il sesso o
l'orientamento sessuale di ciascuno dei partecipanti è irrilevante.

Tuttavia, il termine "condotta sessualmente esplicita" è più ampio dei soli 17
rapporti sessuali. Include anche la zoofilia commessa con un minore, la
masturbazione di un minore, la violenza sado-masochistica in un contesto
sessuale commessa su un minore o l'esibizione lasciva dei genitali o dell'area
pubica di un minore.

In tutti i casi citati, è irrilevante che il comportamento rappresentato sia reale 18
o simulato. L'autore non può quindi sfuggire alla condanna solo perché il
comportamento sessualmente esplicito non ha avuto luogo.

Il secondo tipo di rappresentazione contemplato dall'articolo 9 § 2 CCC 19
riguarda le immagini pornografiche che mostrano una persona
apparentemente minorenni impegnata in comportamenti sessualmente
espliciti (articolo 9 § 2 let. b CCC). Si tratta di immagini che mostrano persone
che hanno appena raggiunto la maggiore età, ma che vengono fatte passare
per minorenni, o che sono chiaramente maggiorenni, ma il cui abbigliamento,
trucco o accessori danno l'impressione di essere minorenni.

Infine, l'articolo 9, paragrafo 2, lettera c), del CCC si riferisce a immagini 20
realistiche che ritraggono un minorenni impegnato in comportamenti
sessualmente espliciti. Quest'ultima ipotesi si applica in particolare ai fumetti
o ai manga, ai fotomontaggi e persino alle immagini create ex novo dai
computer, come può fare l'intelligenza artificiale.

B. Condotte punibili

L'articolo 9 § 1 CCC elenca cinque condotte punibili. L'elenco è esaustivo. 21

- 22 La prima condotta a cui si fa riferimento è la "produzione", cioè la realizzazione, di una rappresentazione di pornografia infantile in vista della sua diffusione per via informatica. Il termine "produzione" comprende tutti gli atti necessari alla produzione di rappresentazioni di pornografia infantile. Si tratta ovviamente in primo luogo della fissazione delle immagini su un supporto di immagini. Tuttavia, comprende anche la preparazione del luogo e delle attrezzature necessarie per produrre le immagini, il ritocco delle immagini una volta fissate su un supporto, il montaggio di fotografie o filmati o anche la creazione di immagini generate al computer. In altre parole, questo comportamento copre tutte le forme di creazione o di editing dei media visivi. In tutti i casi, tuttavia, il materiale deve essere destinato alla distribuzione per via informatica. La creazione di immagini digitali per il proprio consumo non è punibile come produzione, ma solo come possesso (art. 9 § 1 let. e CCC).
- 23 L'articolo 9 § 1 let. b CCC rende poi reato l'offerta o la messa a disposizione di materiale pedopornografico tramite un sistema informatico. Il termine "offerta" si riferisce alla condotta commerciale con cui l'autore del reato informa i propri clienti di avere a disposizione uno o più prodotti e propone loro di acquistarli. Il tipo di contratto (vendita, scambio, donazione, ecc.) è irrilevante. La "messa a disposizione" è un concetto più ampio di quello di "offerta", in quanto non significa necessariamente che l'autore stia compiendo passi attivi per offrire un prodotto ai suoi clienti. Si riferisce a qualsiasi atto che consenta o faciliti l'accesso a una rappresentazione pedopornografica tramite computer. Ciò include la messa online di materiale pedopornografico, ad esempio attraverso la creazione di siti web, nonché la creazione o la compilazione di collegamenti ipertestuali a siti contenenti materiale pedopornografico.
- 24 Un altro reato punibile è la diffusione o la trasmissione di materiale pedopornografico attraverso un sistema informatico. Entrambi i concetti si riferiscono all'invio di dati. La "diffusione" è la distribuzione di materiale pedopornografico a un numero indeterminato di persone che non ne hanno necessariamente fatto richiesta. Per "trasmissione", invece, si intende l'invio a una o più persone specifiche che ne hanno fatto richiesta. La rappresentazione pedopornografica può essere inviata con qualsiasi mezzo elettronico, compresi e-mail, messaggistica istantanea o trasferimento peer-to-peer.

L'articolo 9(d) CCC fa riferimento anche all'"ottenimento di materiale pedopornografico per sé o per un'altra persona tramite un sistema informatico". Questa condotta consiste nell'ottenere attivamente materiale pedopornografico, ad esempio scaricandolo. I dati devono quindi essere stati trasferiti al sistema informatico dell'autore del reato o dall'autore del reato al sistema informatico di una terza persona. Deve esserci un trasferimento di possesso. I dati devono essere ottenuti per via informatica. La consegna a mano o l'invio per posta non rientrano quindi nella Convenzione. 25

Infine, l'ultima condotta punibile è il "possesso di materiale pedopornografico in un sistema informatico o in un supporto informatico" (art. 9 § 1 let. e CCC). La nozione classica di possesso presuppone sia il controllo fisico sull'oggetto sia la volontà di esercitare tale controllo. Nel mondo virtuale, il requisito oggettivo del controllo fisico sull'oggetto deve, a nostro avviso, essere attenuato, nel senso che è sufficiente che il possessore possa accedere liberamente ai suoi dati in qualsiasi momento. Ciò è ovviamente il caso se i dati sono memorizzati su un sistema informatico di proprietà dell'autore, su un supporto di archiviazione dati come un disco rigido esterno o una chiavetta USB, o sulla scheda di memoria di una fotocamera. Tuttavia, l'autore è in possesso dei dati anche se li registra su un server remoto a cui ha accesso o se li salva nel cloud. 26

Per qualche motivo, il fatto di consultare materiale pedopornografico direttamente online, senza appropriarsene, non è stato menzionato e quindi non è punibile. L'assenza di qualsiasi riferimento a tale condotta nell'elenco dell'articolo 9(1) del Codice penale sembra particolarmente sorprendente. Alla luce dell'obiettivo dichiarato di combattere la pornografia infantile, punire il consumo di pornografia infantile sembra altrettanto importante che criminalizzare la produzione di pornografia infantile. Fortunatamente, questa svista è stata corretta dalla Convenzione del Consiglio d'Europa sulla protezione dei bambini contro lo sfruttamento e l'abuso sessuale. Il suo rapporto esplicativo menziona anche che la condotta di cui all'articolo 20, paragrafo 1, lettera f), è intesa a consentire il perseguimento di coloro che visualizzano immagini di bambini su siti web pedopornografici ma che, non scaricandole, sfuggono all'azione penale. 27

C. Illegalità

- 28 L'autore del reato deve agire senza diritto. Questo elemento costitutivo consente alle Parti di creare eccezioni alla punizione penale per gli autori che agiscono per un interesse degno di protezione, simile a quello artistico, medico o scientifico.
- 29 Questa espressione consente anche di escludere dall'ambito di applicazione dell'articolo 9 del TCC le autorità giudiziarie che detengono legittimamente immagini di pornografia infantile sotto forma di sequestro nell'ambito delle indagini e dei processi in corso.
- 30 L'ubiquità degli smartphone, anche nelle mani dei minori, ha portato a diversi abusi. Al giorno d'oggi non è raro che le persone - in particolare le giovani generazioni - si inviino reciprocamente fotografie delle loro parti intime durante la fase di seduzione. Questa pratica pone un problema quando il mittente di tale fotografia è un minore, in quanto questi produce pornografia infantile fotografando la propria area genitale, la trasferisce quando la invia tramite un sistema di messaggistica istantanea e addirittura la possiede se ne conserva una copia sul proprio smartphone. In questa situazione, il minore è paradossalmente sia autore che vittima del reato punito dall'articolo 9 del Codice penale. Nel contesto dell'art. 9 § 2 let. a CCC, riteniamo che le Parti potrebbero prevedere che un minore che scatta una fotografia con una connotazione sessuale di se stesso, la trasmette o la possiede non agisce senza diritto. D'altro canto, il destinatario della comunicazione che chiede di ricevere tale immagine, conoscendo l'età del mittente, agisce chiaramente senza diritto.
- 31 Per quanto riguarda l'articolo 9(2)(b) CCC, l'espressione "senza diritto" potrebbe anche consentire a una Parte di prevedere, ad esempio, che una persona non sia punibile se viene stabilito che l'individuo raffigurato non è un "minore" ai sensi di tale disposizione.

D. Intenzione

- 32 Il reato deve essere commesso intenzionalmente. L'intenzione deve riguardare tutti gli elementi oggettivi del reato. L'autore del reato deve quindi avere la consapevolezza e l'intenzione di produrre, offrire, mettere a disposizione, diffondere, trasmettere, procurare per sé o per terzi o possedere materiale pedopornografico.

Le Parti possono tuttavia adottare uno standard più specifico, nel qual caso si applicherebbe quest'ultimo standard. La responsabilità potrebbe, ad esempio, essere imposta se vi è "conoscenza e controllo" delle informazioni trasmesse o memorizzate. Non è sufficiente, ad esempio, che un fornitore di servizi agisca come intermediario per la trasmissione di tale rappresentazione, attraverso un sito web o una chat room, tra gli altri mezzi, in assenza del dolo richiesto. Inoltre, un fornitore di servizi non è obbligato a monitorare i contenuti per evitare la responsabilità penale. 33

IV. RISERVE

Gli articoli 9 § 3 e 4 del Codice penale consentono alle Parti di limitare la punibilità in tre modi diversi, ossia in relazione all'età dei minori, alla condotta punibile e agli oggetti della prestazione. 34

A. Per quanto riguarda l'età dei minori raffigurati

Nel processo di elaborazione della Convenzione, le Parti hanno convenuto sull'importanza di fissare la maggiore età in modo uniforme. Hanno quindi deciso che il termine "minore" indica qualsiasi persona di età inferiore ai 18 anni. Questo limite è stato fissato alla luce della definizione di "bambino" contenuta nell'articolo 1 della Convenzione delle Nazioni Unite sui diritti del fanciullo. Tuttavia, va sottolineato che questa età si riferisce allo sfruttamento dei bambini come oggetti sessuali. Va quindi distinta dall'età del consenso ai rapporti sessuali. 35

Dato che alcuni Stati hanno fissato un limite di età inferiore nella loro legislazione nazionale sulla pornografia infantile, l'ultima frase del paragrafo 3 consente alle Parti di fissare un limite di età diverso, che in ogni caso non deve essere inferiore a 16 anni. 36

L'unico Stato che si è avvalso di questa possibilità è la Svizzera. Ha fissato il limite di età a 16 anni, in linea con la formulazione dell'ex articolo 197, paragrafi 3 e 3^{bis}, del Codice penale. Tuttavia, il 16 giugno 2010, la Svizzera ha firmato la Convenzione del Consiglio d'Europa sulla protezione dei minori contro lo sfruttamento e l'abuso sessuale. L'articolo 20 di questa convenzione punisce i reati di pornografia infantile. Il concetto di "bambino" a cui si fa riferimento è definito all'art. 3 let. a come qualsiasi persona di età inferiore ai 18 anni. Poiché non è stato possibile formulare alcuna riserva sul limite di età, 37

è stato necessario modificare l'articolo 197 del Codice penale. La nuova formulazione di questa disposizione è entrata in vigore il 1° luglio 2014. Essa corrisponde ora alla definizione generale contenuta nell'art. 9 § 3 del Codice penale. La riserva formulata dalla Svizzera al momento della ratifica della Convenzione non è quindi più pertinente.

B. Condotta punibile

- 38 La Convenzione autorizza inoltre le Parti a limitare l'azione penale rifiutando di perseguire il fatto di ottenere o procurare a terzi immagini pedopornografiche e/o il fatto di possederle.
- 39 Al momento della ratifica della Convenzione, Ucraina, Giappone e Sri Lanka si sono avvalsi di questa possibilità di non perseguire l'ottenimento e il possesso di materiale pedopornografico. Nel 2014, il Giappone ha modificato la propria legislazione e ha criminalizzato il possesso di materiale pedopornografico, così come il procurarselo per altri. Tuttavia, procurarsela da soli non è ancora punibile.
- 40 Israele ha dichiarato di rifiutarsi di perseguire l'ottenimento di materiale pedopornografico.
- 41 L'Argentina ha dichiarato che il possesso di pornografia infantile non è punibile secondo la sua legge nazionale.
- 42 Altri Stati hanno espresso riserve sulla punibilità dell'ottenimento o del possesso di materiale pedopornografico in alcune condizioni specifiche.
- 43 La Danimarca, ad esempio, ha dichiarato che non punirà il possesso di immagini pornografiche che coinvolgono bambini di almeno 15 anni se il minore interessato ha acconsentito a tale possesso.
- 44 Al momento della ratifica della Convenzione, il Montenegro ha specificato che l'ottenimento e il possesso di materiale pedopornografico non è punibile se la persona che appare nel materiale ha almeno 14 anni e ha dato il suo consenso. Questa eccezione è stata successivamente eliminata.

C. Gli oggetti della rappresentazione

- 45 Infine, la Convenzione consente alle Parti di limitare l'azione penale rifiutando di considerare illecite le immagini che ritraggono una persona

apparentemente minorenne impegnata in comportamenti sessualmente espliciti e/o le immagini realistiche che ritraggono un minore impegnato in comportamenti sessualmente espliciti.

Il Principato di Andorra, la Gran Bretagna, l'Argentina, il Cile, gli Stati Uniti d'America, il Giappone, il Perù e lo Sri Lanka hanno dichiarato che non perseguiranno le rappresentazioni di cui all'articolo 9 § 2 lettere b e c CCC. L'Islanda ha formulato una riserva in tal senso al momento della ratifica della Convenzione. Tale riserva, tuttavia, non è più valida, in quanto la legge del 25 giugno 2012 ha introdotto un nuovo articolo 210a nel codice penale islandese, che punisce anche le rappresentazioni di cui all'articolo 9 § 2 lettere b e c CCC. 46

Danimarca, Ungheria, Montenegro, Svizzera e Israele hanno dichiarato di astenersi dal punire le rappresentazioni visive di una persona apparentemente minorenne che si dedica a comportamenti sessualmente espliciti (art. 9 § 2 let. b). La Francia ha espresso una riserva simile, dichiarando che non perseguirà le immagini che ritraggono una persona maggiorenne al momento in cui l'immagine è stata scattata, ma che sembra essere minorenne ed è impegnata in comportamenti sessualmente espliciti. 47

V. CONFRONTO CON IL DIRITTO SVIZZERO

Le condotte e le varie rappresentazioni punibili ai sensi della Convenzione trovano il loro equivalente nel diritto svizzero nell'articolo 197, paragrafi 4 e 5, del Codice penale. Il diritto svizzero è del tutto coerente con l'art. 9 CCC. 48

BIBLIOGRAFIA

Corboz Bernard, *Les infractions en droit suisse*, vol. I, 3^e éd., Berne 2010

Trechsel Stefan/Cramer Dean, in : Trechsel Stefan/Pieth Mark (éditeurs), *Schweizerisches Strafgesetzbuch, Praxiskommentar*, 4. éd., Zurich 2021

Isenring Bernhard/Kessler Martin A., in : Niggli Marcel Alexander/Wiprächtiger Hans (éditeurs), *Basler Kommentar, Strafrecht II*, 4. éd., Bâle 2018

I MATERIALI

Conseil de l'Europe, Explanatory Report to the Convention on Cybercrime, Budapest 23.11.2001, disponible à <https://rm.coe.int/16800cce5b>, visité le 21.1.2024 (cité : Rapport explicatif de la Convention sur la cybercriminalité)

Conseil de l'Europe, Explanatory Report to the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, Lanzarote 25.10.2007, disponible à <https://rm.coe.int/16800d3832>, visité le 21.1.2024 (cité : Rapport explicatif de la Convention du Conseil de l'Europe sur la protection des enfants contre l'exploitation et les abus sexuels)

ATTENZIONE: Questa versione del commentario è una traduzione automatica dell'originale. Il commentario originale è in tedesco. La traduzione è stata effettuata con www.deepl.com. Solo la versione originale fa fede. La forma tradotta del commentario non può essere citata

COMMENTO SU

Art. 11 CCC (Convenzione sulla cibercriminalità [Cybercrime Convention])

Un commentario di Julian Mausbach

CITAZIONE SUGGERITA

Julian Mausbach, Commentario all'art. 11 CCC, in: Damian K. Graf (a cura di), Commentario online alla Convenzione sulla cibercriminalità [Cybercrime Convention]

Breve citazione: OK-Mausbach, Art. 11 CCC N. XXX.

Titolo 5: Altre forme di responsabilità e sanzioni

Art. 11 Tentativo, complicità e istigazione

¹ Le Parti adottano le misure legislative e di altra natura necessarie per definire come reato, nel loro diritto interno, la complicità intenzionale nella perpetrazione di un reato di cui agli articoli 2–10 o l'istigazione intenzionale a tale reato, con l'intento che venga commesso.

² Le Parti adottano le misure legislative e di altra natura necessarie per definire come reato, nel loro diritto interno, il tentativo intenzionale di

commettere un reato di cui agli articoli 3–5, 7, 8, 9 paragrafo 1 lettere a e c.

³ Le Parti possono riservarsi il diritto di non applicare in tutto o in parte il paragrafo 2.

STRUTTURA

I. Ambito di applicazione	130
II. Responsabilità penale per partecipazione (art. 11 cpv. 1)	130
III. Tentativo di reato (art. 11 cpv. 2 e cpv. 3)	131
I Materiali	132

I. AMBITO DI APPLICAZIONE

- 1 L'art. 11 ha lo scopo di stabilire il principio della responsabilità penale per il tentativo e la partecipazione in relazione ai reati definiti dalla Convenzione. Il cpv. 1 parte dal presupposto che la partecipazione intenzionale a un reato intenzionale ai sensi degli artt. 2-10 sia punibile e sanzionabile sia nel senso del favoreggiamento che dell'istigazione.
- 2 Il cpv. 2 limita già la responsabilità penale per i tentativi di reato agli artt. 3-5 e agli artt. 7, 8 e 9 cpv. 1 lett. a e c della Convenzione. Questa limitazione della responsabilità penale per il tentativo ai reati elencati può essere attuata dalle Parti contraenti in modo tale che la responsabilità penale per il tentativo sia esonerata in tutto o in parte (cpv. 3).
- 3 La Svizzera non si è avvalsa della possibilità di limitare il cpv. 3 e pertanto prevede il reato di tentativo collegandolo alla Parte generale del Codice penale.

II. RESPONSABILITÀ PENALE PER PARTECIPAZIONE (ART. 11 CPV. 1)

- 4 L'art. 11 cpv. 1 prevede la responsabilità penale per la partecipazione per gli artt. 2-10. A differenza della Parte generale del Codice penale (artt. 24 e 25 CP), non viene fatta alcuna distinzione tra istigazione e favoreggiamento. Poiché l'attuazione del cpv. 1 è avvenuta direttamente attraverso le disposizioni della Parte Generale del Codice Penale, la forma assunta in tale sede, ad esempio per quanto riguarda il tentativo di reato (art. 24 cpv. 2 CP), si applica anche all'ambito di applicazione della Convenzione e alla relativa attuazione. Non sono previsti requisiti oggettivi che vadano oltre gli artt. 24 e 25 CP e quindi l'attuazione attraverso questi articoli è congruente anche in questo caso.
- 5 La doppia intenzione di partecipare prevista dal cpv. 2 per quanto riguarda l'atto di partecipazione e il reato principale è richiesta anche dalle disposizioni della Parte Generale, per cui non è stata necessaria alcuna integrazione.
- 6 Si rimanda all'aggiunta alla disposizione penale dell'Art. 143bis CP. Per i dettagli, si rimanda al corrispondente commento all'Art. 6. Per quanto

riguarda la questione della partecipazione e del tentativo, va sottolineato che anche dopo la modifica dell'Art. 143bis CP, il tentativo di concorso in un reato principale non (ancora) tentato rimane impunito.

III. TENTATIVO DI REATO (ART. 11 CPV. 2 E CPV. 3)

Il cpv. 2 prevede l'obbligo di estendere la responsabilità penale per tentativo 7 alle disposizioni citate. Non sono specificati criteri oggettivi, né è previsto un reato di tentativo generale. Quest'ultimo aspetto è dovuto in particolare al fatto che gli ordinamenti giuridici di alcune parti contraenti non prevedono un reato di tentativo generale ma graduale. La disposizione adottata promette quindi un'opzione di attuazione che può essere (ed è stata) attuata senza grandi distorsioni nei concetti giuridici fondamentali degli Stati contraenti.

L'attuazione del tentativo di incriminazione è stata effettuata tramite l'art. 22 8 in combinato disposto con l'art. 10 par. Art. 10 cpv. 2 e cpv. 3 CP. Si estende quindi a tutti i reati specificati al cpv. 2. Ciò è dovuto al fatto che la loro attuazione avviene a sua volta attraverso i reati della Parte Speciale del CP, che sono essi stessi almeno reati ai sensi dell'art. 10 cpv. 2 CP.

Sebbene il cpv. 2 non contenga alcun obbligo di estendere il reato di tentativo 9 alle disposizioni non menzionate nel cpv. 2, l'attuazione attraverso gli articoli del Codice penale significa che anche in Svizzera esiste il reato di tentativo per quanto riguarda l'art. 2, l'art. 9 nel suo complesso e l'art. 10 CP. In particolare, con l'inclusione dei reati documentali (art. 251 e segg. CP), dei reati per la tutela del segreto postale e delle telecomunicazioni (art. 321ter CP) e dell'articolo sulla pornografia (art. 197 CP), che a loro volta sono almeno reati, si è verificata un'attuazione che comporta la responsabilità penale per tentativo per gli artt. 2-10. Pertanto, non vi è alcuna dissonanza con il principio del tentativo di responsabilità penale per reati e crimini nel diritto penale svizzero.

Il cpv. 3 prevede la possibilità per le parti contraenti di rinunciare in tutto o in 10 parte alla responsabilità penale per i tentativi. Questa disposizione mira a contrastare eventuali difficoltà di attuazione incontrate dalle parti contraenti. Il margine di manovra così concesso per l'attuazione dovrebbe consentire, per quanto possibile, di ratificare la Convenzione senza modifiche sostanziali dei rispettivi ordinamenti giuridici. In Svizzera non ci si è avvalsi di questa possibilità, nemmeno per quanto riguarda singoli elementi o parti di essi. Ciò

è convincente dal punto di vista del contenuto, in quanto non comporta una rottura con la concezione del tentativo di reato in Svizzera. La disposizione di cui al cpv. 3, che in ultima analisi deve essere intesa come una concessione alla praticabilità dell'attuazione in relazione agli ordinamenti giuridici delle parti contraenti, è stata quindi lasciata senza conseguenze in Svizzera.

I MATERIALI

Botschaft über die Genehmigung und die Umsetzung des Übereinkommens des Europarates über die Cyberkriminalität vom 18.6.2010, BBl 2010 4697 ff., abrufbar unter <https://www.fedlex.admin.ch/eli/fga/2010/813/de>, besucht am 17.10.2023

Europarat, Explanatory Report to the Convention on Cybercrime, Budapest 23.11.2001, abrufbar unter <https://rm.coe.int/16800cce5b>, besucht am 17.10.2023 (zit. Explanatory Report)

ATTENZIONE: Questa versione del commentario è una traduzione automatica dell'originale. Il commentario originale è in tedesco. La traduzione è stata effettuata con www.deepl.com. Solo la versione originale fa fede. La forma tradotta del commentario non può essere citata

COMMENTO SU

Art. 12 CCC (Convenzione sulla cybercriminalità [Cybercrime Convention])

Un commentario di Ugur Gürbüz

CITAZIONE SUGGERITA

Ugur Gürbüz, Commentario all'art. 12 CCC, in: Damian K. Graf (a cura di), Commentario online alla Convenzione sulla cybercriminalità [Cybercrime Convention]

Breve citazione: OK-Gürbüz, art. 12 CCC N. XXX.

Art. 12 Responsabilità delle persone giuridiche

¹ Le Parti adottano le misure legislative e di altra natura necessarie affinché le persone giuridiche possano essere ritenute responsabili di un reato previsto dalla presente Convenzione, commesso per loro conto da una persona fisica che agisce individualmente o in quanto membro di un organo della persona giuridica, e che detiene una posizione dirigenziale al suo interno in virtù di:

a. un potere di rappresentanza della persona giuridica;

- b. una facoltà di assumere decisioni nel nome della persona giuridica;
- c. una facoltà di controllo all'interno della persona giuridica.

² Oltre ai casi già previsti al paragrafo 1, le Parti adottano le misure necessarie affinché una persona giuridica possa essere ritenuta responsabile se la mancanza di sorveglianza o controllo da parte di una persona fisica di cui al paragrafo 1 ha reso possibile la commissione di un reato previsto dalla presente Convenzione per conto della persona giuridica ad opera di una persona fisica che agisce sotto la sua autorità.

³ A seconda dei principi giuridici delle Parti, la responsabilità delle persone giuridiche può essere penale, civile o amministrativa.

⁴ Questa responsabilità non pregiudica la responsabilità penale delle persone fisiche che hanno commesso il reato.

STRUTTURA

I. Introduzione	136
II. Ambito di applicazione e obiettivi	137
A. Paragrafo 1: Per gli atti commessi da persone in posizione di leadership	137
B. Paragrafo 2: violazione dell'obbligo di vigilanza.....	138
C. Paragrafo 3: Tipo di responsabilità	139
D. Paragrafo 4: Responsabilità individuale.....	139
III. Norme di diritto penale comparabili in Svizzera	140
A. Sanzioni e misure penali previste dal CP svizzero	140
B. Art. 102 cpv. 1 CP: Responsabilità delle società controllate	140
C. Art. 102 cpv. 2 CP: Responsabilità primaria	142
D. Disposizioni di diritto penale amministrativo	142
1. Art. 6 VStrR: responsabilità del committente.....	143
2. Art. 7 VStrR: responsabilità dell'impresa	143
IV. Attuazione dell'aspetto penale in Svizzera	144
V. Norme di diritto civile e amministrativo comparabili in Svizzera	145
VI. Attuazione dell'aspetto del diritto civile e amministrativo in Svizzera	146
Bibliografia	146
I Materiali	147

I. INTRODUZIONE

- 1 Per decenni, il principio "**societas delinquere non potest**", che ha origine nel diritto romano, è stato considerato una regola immutabile nell'Europa continentale, concentrando il diritto penale sull'individuo ed esentando le società dalla responsabilità penale. L'idea di un sistema giuridico privo di responsabilità penale diretta delle imprese è diventata obsoleta quando l'economia è diventata sempre più caratterizzata da strutture aziendali più complesse e da divisioni globali del lavoro, aumentando così il potenziale di abuso e la pericolosità e dannosità di qualsiasi comportamento aziendale scorretto. In Europa, i Paesi Bassi nel 1976, la Francia nel 1994 e la Danimarca nel 1996 hanno introdotto la criminalizzazione delle società nei loro codici penali. In Svizzera, il diritto penale societario è disciplinato nel Codice penale dal 1° ottobre 2003, ma la Svizzera è ancora considerata uno dei Paesi pionieri a livello internazionale per quanto riguarda l'introduzione della responsabilità penale per le persone giuridiche. Anche prima della sua introduzione nel Codice Penale, gli articoli 6 e 7 della Legge sulle infrazioni amministrative (VStrR) potevano essere invocati dal 1974 per i reati nelle operazioni commerciali in conformità con l'art. 26 LCSL (Legge federale contro la concorrenza sleale). Tuttavia, queste disposizioni sono state considerate come eccezioni al principio, allora generalmente riconosciuto, della non perseguibilità delle persone giuridiche e non sono state incluse nel diritto penale.
- 2 Con l'introduzione della Convenzione sulla criminalità informatica del Consiglio d'Europa, le parti contraenti, seguendo la **tendenza europea**, hanno inserito nell'art. 12 CCC norme sulla responsabilità delle persone giuridiche identiche a quelle contenute nelle disposizioni penali, in gran parte identiche, della Convenzione penale sulla corruzione, ossia la responsabilità per i reati commessi dai loro organi e altri dipendenti. Gli Stati contraenti sono inoltre tenuti, ai sensi dell'art. 12 CCC, a garantire che le persone giuridiche siano soggette a sanzioni o misure adeguate, comprese le sanzioni pecuniarie. La Convenzione sulla criminalità informatica ha tutelato anche il principio secondo cui le società non possono rendersi perseguibili da sole.

II. AMBITO DI APPLICAZIONE E OBIETTIVI

La **responsabilità delle persone giuridiche** ai sensi dell'articolo 12 mira, da un lato, a ritenere le società responsabili per i reati commessi da persone in posizione dirigenziale, a condizione che tali reati siano commessi a vantaggio della persona giuridica (paragrafo 1). Dall'altro lato, la disposizione prevede la responsabilità delle persone in posizione dirigenziale che hanno omesso di supervisionare o controllare i dipendenti o gli agenti e tale omissione facilita la commissione di un reato da parte dei dipendenti o degli agenti come definito dalla Convenzione (paragrafo 2). La Convenzione lascia alle parti contraenti la facoltà di decidere se disciplinare la responsabilità della persona giuridica in base al diritto civile, amministrativo o penale (paragrafo 3). Essa stabilisce inoltre che la responsabilità della persona giuridica non impedisce l'eventuale responsabilità penale della persona fisica che ha commesso il reato (paragrafo 4).

A. Paragrafo 1: Per gli atti commessi da persone in posizione di leadership

L'art. 12 cpv. 1 del CDC obbliga le parti contraenti a stabilire la responsabilità della persona giuridica per i reati commessi da persone in posizione di comando all'interno dell'azienda o che vi partecipano in qualità di istigatori o complici. La disposizione stabilisce la **responsabilità causale** e comprende **quattro elementi**:

a) La Convenzione richiede un reato contro le **norme penali formulate negli articoli da 2 a 10 della Convenzione**, vale a dire l'accesso illecito (art. 2), l'intercettazione illecita (art. 3), l'interferenza con i dati (art. 4), l'interferenza con un sistema (art. 5), l'uso improprio di dispositivi (art. 5), uso improprio di dispositivi (art. 6), contraffazione informatica (art. 7), frode informatica (art. 8), reati di pornografia infantile (art. 9) e violazione del diritto d'autore e dei diritti connessi (art. 10).

b) La responsabilità penale prevista dal testo della Convenzione è limitata ai reati **commessi a beneficio della persona giuridica**. Il criterio "a vantaggio della persona giuridica" stabilisce un legame tra il reato e la persona giuridica. L'ambito di applicazione è limitato ai reati commessi a beneficio di una persona giuridica. Tale vantaggio può essere finanziario o di altro tipo. I benefici finanziari diretti comprendono, tra l'altro, i proventi ottenuti da reati

che arricchiscono la persona giuridica o le fanno risparmiare una spesa. Esiste un beneficio di tipo diverso se il beneficio per la persona giuridica non è (principalmente) finanziario, ad esempio se la persona giuridica riceve ordini come risultato della corruzione. La Convenzione non contiene una definizione giuridica del termine persona giuridica. Nella definizione dell'articolo 12, è stata utilizzata l'interpretazione storica ed europea del termine "persona giuridica", secondo la quale esso comprende qualsiasi soggetto giuridico che abbia lo status di persona giuridica ai sensi della legge applicabile, ad eccezione degli Stati o di altri enti pubblici nell'esercizio dei diritti sovrani e delle organizzazioni internazionali pubbliche.

- 7 c) In conformità ai principi di diritto privato secondo cui le persone giuridiche possono agire solo attraverso i propri organi, gli atti degli organi sono atti diretti della persona giuridica e la persona giuridica è responsabile degli atti degli

organi nei confronti dei terzi danneggiati, la Convenzione presuppone la **commissione del reato da parte di una persona fisica** che ricopre una **posizione preminente** all'interno della persona giuridica. Secondo l'elenco di cui alle lettere da a a c, sono comprese le persone fisiche che traggono la loro funzione di direzione e di leadership da un potere di rappresentanza, di decisione o di controllo. Il testo della Convenzione richiede quindi che la responsabilità delle persone giuridiche sia definita come un reato speciale, senza presupporre che l'autore del reato abbia una funzione esecutiva formale.

- 8 d) Inoltre, la Convenzione impone agli Stati contraenti di garantire che la persona fisica agisca nell'ambito dei poteri conferitigli nell'esercizio di **un'attività commerciale autorizzata**, ovvero agisca nell'ambito del potere di rappresentanza, decisione o controllo conferitole dalla persona giuridica, al fine di far scattare la responsabilità della persona giuridica ai sensi dell'art. 12 cpv. 1 CPC.

B. Paragrafo 2: violazione dell'obbligo di vigilanza

- 9 L'art. 12 cpv. 2 del CDC obbliga gli Stati contraenti a ritenere responsabili le imprese
- a) se le persone fisiche di cui al cpv. 1 lett. da a a c **violano il loro dovere di vigilanza sui dipendenti subordinati attraverso una sorveglianza e un**

controllo inadeguati,

b) che poi commettono un reato come conseguenza causale di questa violazione ai sensi dell'**art. 2-10 del Codice Civile**

c) commettono un reato a **vantaggio della persona giuridica** .

Il paragrafo 2 estende quindi la responsabilità della persona giuridica agli atti 10 commessi da persone che commettono un reato in qualità di dipendenti **senza una posizione dirigenziale** nella persona giuridica e il reato è stato reso possibile dal fatto che il dirigente non ha adeguatamente supervisionato il dipendente subordinato.

Si ritiene che l'**omessa vigilanza** si sia verificata se non sono state adottate 11 misure adeguate e appropriate per prevenire atti criminali a favore della persona giuridica da parte di dipendenti o agenti. Il tipo e l'intensità dell'obbligo di vigilanza dipendono dal tipo di azienda, dalle sue dimensioni, dagli standard di sicurezza e dalle pratiche commerciali. L'obbligo di vigilanza non comporta un obbligo di controllo generale.

C. Paragrafo 3: Tipo di responsabilità

L'art. 12 cpv. 3 CCC è stato inserito nella Convenzione per tenere conto il più 12 possibile dei principi giuridici nazionali degli Stati contraenti. Secondo questa disposizione della Convenzione, la **responsabilità delle persone giuridiche** può essere **penale, civile o amministrativa**. Gli Stati contraenti devono garantire che le loro sanzioni o misure penali o non penali contro le persone giuridiche soddisfino i criteri dell'art. 13 cpv. 2 CPC, secondo cui devono essere effettive, proporzionate e dissuasive e includere sanzioni pecuniarie.

D. Paragrafo 4: Responsabilità individuale

L'art. 12 cpv. 4 CPC chiarisce che la responsabilità delle persone giuridiche 13 **non esclude la responsabilità individuale di una persona fisica**. Questa disposizione non obbliga gli Stati contraenti a introdurre una responsabilità penale parallela.

III. NORME DI DIRITTO PENALE COMPARABILI IN SVIZZERA

A. Sanzioni e misure penali previste dal CP svizzero

- 14 La responsabilità penale delle imprese è stata introdotta nel Codice penale svizzero il 1° ottobre 2003. Le motivazioni sono state la paura della criminalità organizzata, il timore di grandi pericoli causati dall'uomo e la firma della "Convenzione sulla lotta alla corruzione di pubblici ufficiali stranieri nelle transazioni commerciali internazionali". Ratificando questa **Convenzione OCSE**, la Svizzera si è impegnata, ai sensi dell'art. 2, ad adottare le misure necessarie per stabilire la responsabilità delle persone giuridiche per la corruzione di un pubblico ufficiale straniero in conformità con i suoi principi giuridici.

B. Art. 102 cpv. 1 CP: Responsabilità delle società controllate

- 15 Ai sensi dell'art. 102 cpv. 1 CP, i reati o gli illeciti - ma non le violazioni - sono attribuiti a una società se un reato o un illecito è commesso nella "società nello svolgimento di attività commerciali nell'ambito dello scopo della società" e "questo atto non può essere attribuito a una persona fisica specifica a causa di un'organizzazione inadeguata della società". La società è quindi soggetta a responsabilità penale sussidiaria in caso di **organizzazione** difettosa.
- 16 L'accusa nei confronti della società è di
- a) è stato commesso un **reato o un illecito** di diritto svizzero ai sensi dell'art. 10 CP **come reato istigatorio**
 - b) il reato è stato commesso **all'interno di una società** e l'autore del reato deve essere gerarchicamente o organizzativamente integrato nella società stessa
 - c) il reato presupposto è stato commesso "**nell'ambito dell'attività aziendale**", il che richiede un collegamento funzionale tra il reato presupposto e l'attività aziendale, vale a dire un'attività economica minima correlata alle attività dell'azienda e che quindi comprenda l'azione con potere di rappresentanza, di decisione o di controllo richiesta dall'Art. 12 CCC,

d) il reato è stato commesso **nell'ambito dell'oggetto sociale** che, secondo l'opinione prevalente, giustifica una limitazione ai rischi tipici dell'attività,

e) l'azienda è responsabile del fatto che le autorità penali **non sono in grado** di identificare una **persona fisica responsabile** a causa di un'organizzazione inadeguata.

Finché la responsabilità delle persone giuridiche

17

- da un lato, ai sensi dell'art. 12 par. 1 della Convenzione, l'obiettivo è quello di ritenere le società responsabili per i reati commessi da persone in posizione dirigenziale, a condizione che tali reati siano commessi a beneficio della persona giuridica,
- e dall'altro lato, secondo l'art. 12 cpv. 2 CPC, le persone in posizione dirigenziale che hanno omesso di sorvegliare o controllare i dipendenti o gli agenti e tale omissione facilita un reato da parte dei dipendenti o degli agenti come descritto nella Convenzione,

Entrambe le varianti di reato trovano un equivalente di ampia portata nella responsabilità sussidiaria dell'impresa ai sensi dell'art. 102 cpv. 1 CP. Questa disposizione copre **tutti i reati previsti dalla Convenzione Cyber** senza elencarli esplicitamente.

La Convenzione si limita ai reati di cui agli artt. 2-10 CPC commessi a beneficio della persona giuridica e dai suoi rappresentanti. La responsabilità ai sensi del CP, invece, si applica a qualsiasi reato o illecito commesso da una persona nel corso di un'attività commerciale nell'ambito dell'oggetto sociale. Rispetto al testo della Convenzione, la responsabilità ai sensi del Codice penale svizzero si estende quindi ulteriormente, poiché il CP **non** richiede un **reato commesso a favore della persona giuridica come criterio** per la responsabilità societaria.

18

L'art. 102 cpv. 1 CP, secondo cui la persona giuridica può essere punita solo se il reato non può essere attribuito a una persona fisica, e l'art. 12 cpv. 4 CP, secondo cui la responsabilità penale della persona giuridica non deve influire sulla responsabilità dell'autore, non si contraddicono perché la **responsabilità penale delle persone fisiche che agiscono non è esclusa dalla responsabilità sussidiaria della società**. In Svizzera, è persino

19

possibile punire la persona fisica oltre alla persona giuridica se l'organizzazione difettosa della società è imputabile a una persona fisica e questa persona può essere identificata solo dopo la condanna della società.

- 20 L'art. 102 cpv. 1 CP prevede come sanzione una **multa fino a cinque milioni di franchi svizzeri**, il che corrisponde al testo della Convenzione all'art. 13 cpv. 2, secondo cui gli Stati contraenti devono imporre sanzioni pecuniarie.

C. Art. 102 cpv. 2 CP: Responsabilità primaria

- 21 A prescindere dalla responsabilità penale delle persone fisiche, dall'1.10. 2003, una **società è responsabile in via principale** se viene commesso un reato ai sensi degli articoli ^{260ter} CP (organizzazione criminale), ^{260quinquies} CP (finanziamento del terrorismo), ^{305bis} CP (riciclaggio di denaro), ^{322ter} CP (corruzione di pubblici ufficiali svizzeri), ^{322quinquies} CP (concessione di vantaggi), ^{322septies} paragrafo 1 CP (corruzione di pubblici ufficiali stranieri) o ^{322octies} CP (corruzione) e l'azienda non ha adottato tutte le precauzioni organizzative necessarie e ragionevoli per prevenire tale reato. La **violazione del dovere** consiste nell'inosservanza degli obblighi organizzativi che facilitano i reati elencati in modo esaustivo. Ai sensi dell'art. 102 cpv. 2 CP, il reato è punito in aggiunta alle pene previste per le persone fisiche.
- 22 Nessuno dei reati di cui agli artt. 2-10 CP è incluso nel catalogo dei reati di cui all'art. 102 cpv. 2 CP, motivo per cui la responsabilità delle persone giuridiche di cui all'art. 12 CP è priva di significato rispetto alla responsabilità penale primaria delle società. Ne consegue che, in base alle disposizioni di legge vigenti, in Svizzera **non è possibile attribuire direttamente la colpa di terzi a una società** in relazione alle norme penali formulate negli artt. 2-10 CCC.

D. Disposizioni di diritto penale amministrativo

- 23 Prima dell'introduzione della responsabilità penale delle imprese e della disposizione sull'imputazione (art. 29 CP) nel diritto penale fondamentale e anche prima della ratifica della Convenzione sulla criminalità informatica, in Svizzera le persone fisiche e giuridiche erano ritenute responsabili per i reati commessi nell'ambito di operazioni commerciali ai sensi della Legge federale sul diritto penale amministrativo. Le corrispondenti disposizioni del diritto penale amministrativo **continuano ad essere applicate**: l'art. 6 della VStrR

punisce le persone fisiche che hanno un rapporto particolare con l'esercizio commerciale. L'art. 7 della VStrR riguarda la responsabilità penale delle persone giuridiche. Ci possono essere sovrapposizioni tra le disposizioni del CP e del VStrR. Gli artt. 6 e 7 VStrR sono applicabili fintanto che le leggi fanno esplicito riferimento a una delle disposizioni o al diritto penale amministrativo nel suo complesso.

1. Art. 6 VStrR: responsabilità del committente

L'oggetto della responsabilità penale ai sensi dell'art. 6 VStrR è sempre una **persona fisica**. Se i reati sono commessi durante la gestione degli affari di una persona giuridica, di una società in nome collettivo o in accomandita, di un'impresa individuale o di un gruppo di persone senza personalità giuridica o comunque nell'ambito di un'attività commerciale o di un incarico ufficiale, il paragrafo 1 stabilisce che la disposizione penale si applica alla persona fisica che ha commesso il reato. I paragrafi 2 e 3 specificano che il committente, il datore di lavoro, il preponente, il rappresentante o anche l'organo e il membro dell'organo, il socio amministratore, il liquidatore e la persona effettivamente responsabile sono da ritenersi responsabili nella misura in cui abbiano intenzionalmente o per negligenza omesso di evitare un reato commesso dal subordinato, dall'agente o dal rappresentante o di annullarne gli effetti in violazione di un dovere legale. L'articolo 6 è un reato di omissione in violazione di un dovere legale. La responsabilità penale amministrativa del committente derivante dall'articolo 6 limita notevolmente l'ambito di applicazione della responsabilità penale sussidiaria dell'azienda ai sensi dell'art. 102 cpv. 1 CP e scagiona l'azienda in quanto consente di attribuire il reato a una persona fisica. 24

2. Art. 7 VStrR: responsabilità dell'impresa

L'art. 7 VStrR prevede la responsabilità penale sussidiaria della persona giuridica nel diritto penale amministrativo. La disposizione mira a ridurre lo sforzo investigativo delle autorità di perseguimento penale **nel caso di reati minori**, in conformità al principio di moderata opportunità. Allo stesso tempo, contraddice il principio dell'accertamento della verità materiale e il principio di legalità. Ai sensi dell'art. 7 VStrR, il procedimento penale nei confronti di una persona fisica può essere archiviato e la persona giuridica, la società in nome collettivo o in accomandita o la ditta individuale può essere condannata al pagamento di una multa al suo posto se sono soddisfatte le 25

seguenti condizioni:

- a) il reato è stato commesso nell'ambito dell'attività commerciale
- b) è possibile una multa fino a un massimo di CHF 5.000,00 e
- c) l'indagine sul singolo autore del reato comporterebbe uno sforzo investigativo sproporzionato.

Se l'autore del reato è una persona fisica, l'applicazione dell'art. 7 VStrR è esclusa. La disposizione non sostituisce l'art. 102 cpv. 1 CP nel diritto penale amministrativo. A causa del loro diverso contenuto normativo, entrambe le norme possono essere applicate.

IV. ATTUAZIONE DELL'ASPETTO PENALE IN SVIZZERA

- 26 Data l'**ampia copertura del contenuto della Convenzione** da parte dell'art. 102 cpv. 1 CP, il legislatore si è giustamente astenuto dall'imporre la responsabilità primaria delle imprese in ambito penale in relazione all'art. 12 CP e alla relativa estensione del campo di applicazione. Sebbene la Convenzione sancisca una responsabilità parallela dell'impresa, che in Svizzera può essere garantita solo a livello penale attraverso la responsabilità penale primaria dell'impresa ai sensi dell'art. 102 cpv. 2 CP, essa non impone agli Stati contraenti di regolamentare la responsabilità penale delle imprese. L'art. 12 della Convenzione non richiede la creazione di una disposizione penale in senso stretto, bensì, al cpv. 3, lascia agli Stati contraenti la possibilità di disciplinare in alternativa la responsabilità della persona giuridica nell'ambito del diritto civile o amministrativo. Poiché la responsabilità sussidiaria di cui all'art. 102 cpv. 1 CP copre tutti i reati di cui agli artt. 2-10 CP, soprattutto perché garantisce che i reati e gli illeciti commessi a vantaggio di un'impresa non restino impuniti, il legislatore ha correttamente ritenuto che una responsabilità primaria più completa andasse oltre il minimo richiesto dalla Convenzione. Sulla base dell'art. 2 VStrR, secondo cui le disposizioni del diritto penale societario del CP si applicano anche al diritto penale amministrativo, a meno che la VStrR stessa o la singola legge amministrativa non dispongano diversamente, ma anche sulla base dell'art. 7 VStrR, secondo cui le associazioni di personale possono essere punite al posto di singoli autori di reato difficilmente identificabili, la responsabilità delle persone

giuridiche è garantita anche nel caso di reati per violazione di leggi federali come la legge sul diritto d'autore.

Contrariamente alla formulazione e allo scopo dell'art. 12 cpv. 1 CP, il ²⁷ legislatore svizzero non ha configurato l'art. 102 CP come un reato di responsabilità causale. Mentre secondo l'art. 12 cpv. 1 CP una persona giuridica dovrebbe assumersi il rischio di responsabilità per un reato commesso all'interno dell'azienda indipendentemente dalla sua colpa, l'art. 102 CP presuppone una colpa organizzativa per la responsabilità penale della persona giuridica. Nonostante questa differenza, la Svizzera soddisfa comunque i requisiti dell'art. 12 CPC perché "responsabilità" ai sensi della Convenzione non significa necessariamente responsabilità penale della persona giuridica (cfr. art. 12 cpv. 3 CPC).

V. NORME DI DIRITTO CIVILE E AMMINISTRATIVO COMPARABILI IN SVIZZERA

L'ordinamento giuridico svizzero riconosce diversi strumenti di responsabilità ²⁸ per danni e prevenzione di danni futuri nell'ambito del diritto civile e amministrativo. Oltre alle **norme di responsabilità e alle misure organizzative** di diritto civile, occorre fare riferimento anche agli **strumenti di vigilanza** delle autorità.

In particolare, questi strumenti includono i seguenti (non esaustivi): ²⁹

- Scioglimento dell'associazione da parte del tribunale ai sensi dell'art. 78 CC se lo scopo dell'associazione è illegale o immorale;
- Cancellazione della fondazione da parte dell'autorità federale o cantonale competente ai sensi dell'Art. 88 del CC se il suo scopo è diventato illegale o immorale;
- Responsabilità della società derivante dalla responsabilità del committente ai sensi dell'art. 55 CO;
- Responsabilità della società per le persone ausiliarie ai sensi dell'art. 101 CO;
- Responsabilità della società per danni derivanti da atti non autorizzati commessi da un azionista nell'esercizio della sua attività ai sensi dell'art. 567 cpv. 3 CO;

- Responsabilità della società per danni derivanti da atti non autorizzati commessi da un liquidatore nell'esercizio delle sue funzioni ai sensi dell'art. 586 CO e dell'art. 743 CO;
- Responsabilità della società per danni derivanti da atti non autorizzati commessi da una persona autorizzata a gestire o rappresentare la società nell'esercizio delle proprie funzioni ai sensi degli artt. 722 CO e 817 CO;
- scioglimento della società in caso di carenze organizzative ai sensi dell'art. 731b CO;
- Responsabilità della cooperativa per danni derivanti da atti non autorizzati commessi da una persona autorizzata a gestire o rappresentare la società nell'ambito delle sue attività commerciali ai sensi dell'art. 899 CO;
- sanzioni amministrative comminate dall'Autorità di vigilanza sui mercati finanziari ai sensi della Legge sulla vigilanza dei mercati finanziari.

VI. ATTUAZIONE DELL'ASPETTO DEL DIRITTO CIVILE E AMMINISTRATIVO IN SVIZZERA

- 30 Il diritto civile e amministrativo svizzero prevede un **gran numero di sanzioni e misure** contro le società per atti non autorizzati nell'ambito di un'attività commerciale. Finché le società sono gestite per l'esercizio di un'attività commerciale e non esclusivamente per commettere reati, le sanzioni e le misure previste dal diritto civile e amministrativo sono generalmente sufficienti a garantire le sanzioni efficaci e dissuasive richieste dall'art. 13 cpv. 2 del Codice civile.

BIBLIOGRAFIA

Ackermann Jürg-Beat, Wirtschaftsstrafrecht der Schweiz, 2. Aufl., Bern 2021 (zit. Ackermann, Bearbeiter/in, § ... N ...).

Donatsch Andreas/Heimgartner Stefan/Isenring Bernhard/Maurer Hans/Riesen-Kupper Marcel/Weder Ulrich (Hrsg.), StGB/JStG Kommentar, Mit weiteren Erlassen und Kommentaren zu den Strafbestimmungen des SVG, BetmG, AIG und OBG, 21. Aufl., Zürich 2022 (zit. StGB/JStG Kommentar, Art. ... StGB N ...).

Forster Matthias, Die strafrechtliche Verantwortlichkeit des Unternehmens nach Art. 102 StGB, Bern 2006.

Frank Friedrich/Eicker Andreas/Markwalder Nora/Achermann Jonas (Hrsg.), Basler Kommentar zum Verwaltungsstrafrecht, 1. Aufl., Basel 2020 (zit. BSK-Bearbeiter/in, Art. ... VStrR N ...).

Heine Günter, Europäische Entwicklung bei der strafrechtlichen Verantwortlichkeit von Wirtschaftsunternehmen und deren Führungskräften, ZStrR 119 (2001), S. 22 ff.

Jean-Richard-dit-Bressel Marc, Das Desorganisationsdelikt in Finanzdienstleistungsunternehmen, SZW 2022, S. 572-585.

Niggli Marcel Alexander/Wiprächtiger Hans (Hrsg.), Basler Kommentar zum Strafrecht I, Art. 1-136 StGB, 4. Aufl., Basel 2019 (zit. BSK-Bearbeiter/in, Art. ... StGB N ...).

Riklin Franz, Schweizerisches Strafrecht – Allgemeiner Teil I – Verbrechenslehre, 3. Aufl., Zürich/Basel/Genf 2007.

I MATERIALI

Botschaft über die Genehmigung und die Umsetzung des Übereinkommens des Europarates über die Cyberkriminalität vom 18.6.2010, BBl 2010 4697 ff., abrufbar unter <https://www.fedlex.admin.ch/eli/fga/2010/813/de>, besucht am 30.4.2024.

Botschaft zur Änderung des Schweizerischen Strafgesetzbuches (Allgemeine Bestimmungen, Einführung und Anwendung des Gesetzes) und des Militärstrafgesetzes sowie zu einem Bundesgesetz über das Jugendstrafrecht vom 21.9.1998, BBl 1999 II 1979 ff., abrufbar unter https://www.fedlex.admin.ch/eli/fga/1999/1_1979_1787_1669/de, besucht am 30.4.2024.

Bundesamt für Justiz, Vernehmlassungsentwurf, Genehmigung und Umsetzung des Übereinkommens des Europarates über die Cyberkriminalität, Vorentwurf und Erläuternder Bericht, Bern, März 2009, abrufbar unter <https://www.bj.admin.ch/bj/de/home/sicherheit/gesetzgebung/archiv/cybercrime-europarat.html>, besucht am 30.4.2024.

Dänischen Strafgesetzbuch, abrufbar unter <https://www.retsinformation.dk/eli/lta/2022/1360>, besucht am 30.4.2024.

Erläuternder Bericht zu dem Zweiten Protokoll zum Übereinkommen über den Schutz der finanziellen Interessen der Europäischen Gemeinschaften (vom Rat angenommen am 12.3.1999), abrufbar unter <https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A51999XG0331>, besucht am 30.4.2024.

Französisches Strafgesetzbuch, abrufbar unter https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006070719/2024-01-19, besucht am 30.4.2024.

Niederländischen Strafgesetzbuch, abrufbar unter <https://wetten.overheid.nl/BWBR0001854>, besucht am 30.4.2024.

Richtlinie 2013/40/EU des Europäischen Parlaments und des Rates vom 12.8.2013 über Angriffe auf Informationssysteme und zur Ersetzung des Rahmenbeschlusses 2005/222/JI des Rates, abrufbar unter <https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32013L0040>, besucht am 30.4.2024.

ATTENZIONE: Questa versione del commentario è una traduzione automatica dell'originale. Il commentario originale è in tedesco. La traduzione è stata effettuata con www.deepl.com. Solo la versione originale fa fede. La forma tradotta del commentario non può essere citata

COMMENTO SU

Art. 16 CCC (Convenzione sulla cibercriminalità [Cybercrime Convention])

Un commentario di Ugur Gürbüz

CITAZIONE SUGGERITA

Ugur Gürbüz, Commentario all'art. 16 CCC, in: Damian K. Graf (a cura di), Commentario online alla Convenzione sulla cibercriminalità [Cybercrime Convention]

Breve citazione: OK-Gürbüz, art. 16 CCC N. XXX.

Titolo 2: Conservazione rapida di dati informatici memorizzati

Art. 16 Conservazione rapida di dati informatici memorizzati

¹ Le Parti adottano le misure legislative e di altra natura necessarie per consentire alle autorità competenti di ordinare od ottenere in altro modo la conservazione rapida di specifici dati informatici, inclusi i dati relativi al traffico, memorizzati attraverso un sistema informatico, soprattutto quando vi è motivo di ritenere che tali dati siano particolarmente esposti a perdita o alterazione.

² Quando le Parti applicano il paragrafo 1 ingiungendo a un soggetto di conservare specifici dati informatici memorizzati che si trovano in suo possesso o sotto il suo controllo, adottano le misure legislative e di altra natura necessarie per obbligare detto soggetto a conservare e salvaguardare l'integrità dei dati per il periodo di tempo richiesto – al massimo 90 giorni – per consentire alle autorità competenti di ottenere la loro trasmissione. Le Parti possono prevedere il successivo rinnovo di tale ingiunzione.

³ Le Parti adottano le misure legislative e di altra natura necessarie per obbligare il custode dei dati o la persona incaricata di conservarli a mantenere il segreto sulle procedure intraprese per il periodo di tempo previsto dal loro diritto interno.

⁴ Le facoltà e le procedure di cui al presente articolo sono subordinate agli articoli 14 e 15.

STRUTTURA

I. Introduzione	152
II. Ambito di applicazione e obiettivi	152
A. Cpv. 1: immediata conservazione dei dati informatici	153
B. Cpv. 2: Salvataggio dei dati mediante ordine di conservazione	154
C. Cpv. 3: Obbligo di segretezza.....	155
D. Cpv. 4	155
III. Attuazione in Svizzera	155
A. Salvaguardia da parte delle autorità di perseguimento penale	156
B. Richiesta di conservazione a persone	157
C. Mancanza di disposizioni legislative in materia di ordine di conservazione	158
D. Blocco della conservazione da parte del Tribunale federale in caso di richiesta di sigillatura valida	159
Bibliografia	161
I materiali.....	161

I. INTRODUZIONE

- 1 Il fatto che i criminali informatici professionisti e competenti utilizzino sempre più spesso le tecnologie più recenti e Internet per i loro scopi illegali pone le autorità di fronte a sfide sempre più impegnative. Tuttavia, le possibilità di abuso tecnico non garantiscono una sicurezza permanente e assoluta ai criminali, purché le autorità agiscano in modo mirato. Infatti, **sui supporti dati e su Internet vengono lasciate tracce**: ogni azione eseguita online, ad esempio la visita di un sito web, la pubblicazione sui social media o gli acquisti online, genera dati che vengono memorizzati e possono essere tracciati. Creando immagini dei supporti dati sequestrati è possibile recuperare i dati cancellati e non sovrascritti. Tali dati, anche se memorizzati solo temporaneamente, possono essere utili alle autorità di polizia per identificare gli autori di reati, chiarire il reato o attuare misure di sorveglianza, a condizione che vengano salvati in tempo utile.
- 2 Il fatto che **i dati informatici** siano stati **memorizzati** e siano ancora **disponibili** al momento delle indagini in corso dipende, da un lato, dal comportamento del titolare dei dati in materia di cancellazione e, dall'altro, dalle disposizioni sulla protezione dei dati dello Stato contraente interessato.

II. AMBITO DI APPLICAZIONE E OBIETTIVI

- 3 A causa della loro natura volatile, i dati informatici sono facili da manipolare, modificare e cancellare. Il rischio di perdita o distruzione dei dati è quindi elevato nella pratica. Al fine di non rendere la conservazione di tali dati informatici e dei dati di connessione nei procedimenti penali nazionali dipendente da lunghi processi di raccolta delle prove, ma di impedire tempestivamente la cancellazione e la modifica dei dati rilevanti ai fini probatori mediante un provvedimento di conservazione e di aumentare così l'efficacia dell'azione penale per i reati descritti più dettagliatamente nella Convenzione sulla criminalità informatica, gli Stati contraenti si sono impegnati ad adottare le misure legislative necessarie a livello nazionale. La procedura per garantire la conservazione immediata e tempestiva dei dati informatici memorizzati è denominata in pratica «**procedura di congelamento rapido**». La procedura di congelamento rapido non deve essere confusa con la conservazione immediata dei dati in un contesto

transfrontaliero, la cosiddetta richiesta di conservazione, disciplinata dall'articolo 29 CCC.

L'articolo 16 CCC disciplina la **salvataggio immediato dei dati**, ma non 4
autorizza di per sé gli Stati contraenti a ordinare la consegna dei dati o a prenderne visione, a meno che una norma di competenza interna non lo consenta espressamente. La consegna dei dati è disciplinata dall'articolo 18 CCC, mentre la perquisizione e il sequestro sono trattati nell'articolo 19 CCC.

A. Cpv. 1: immediata conservazione dei dati informatici

L'art. 16 cpv. 1 CCC garantisce la rapida conservazione dei dati informatici 5
all'interno di uno Stato contraente al fine di contrastare il rischio di occultamento dovuto alla volatilità dei dati informatici. I dati devono essere protetti «*da qualsiasi cosa che possa alterarne o deteriorarne la qualità o lo stato*» e quindi in modo completo da modifiche, deterioramenti o cancellazioni. Per salvataggio si intende la **conservazione provvisoria dei dati** e non il rifiuto dell'accesso ai dati. Gli utenti legittimi devono poter continuare a utilizzare i dati o le loro copie, a meno che non debbano essere sequestrati ai sensi dell'articolo 19 CCC.

L'articolo 16 CCC non obbliga gli Stati contraenti a limitare l'offerta o l'utilizzo 6
di servizi, né a introdurre nuove possibilità tecniche per la conservazione e la raccolta di dati. La disposizione non comporta quindi un obbligo di conservazione dei dati. Essa mira semplicemente a garantire che gli Stati contraenti possano disporre a livello nazionale una **protezione accelerata** dei dati informatici memorizzati al fine di sostenersi reciprocamente a livello internazionale.

La **configurazione concreta** delle misure di sicurezza è lasciata alle parti 7
contraenti. Nella pratica sono possibili due opzioni: la conservazione dei dati originali e la creazione di copie identiche dei dati.

Secondo il testo dell'art. 16 cpv. 1 CCC, la conservazione riguarda 8
«*determinati dati informatici, compresi i dati relativi al traffico, che sono stati memorizzati mediante un sistema informatico*». Sono compresi tutti i tipi di dati informatici già raccolti e memorizzati dai titolari dei dati o dai fornitori di servizi, i cosiddetti «**stored computer data**». Sono esplicitamente menzionati anche i dati di connessione e di traffico, i cosiddetti «*traffic data*». Il riferimento ai dati di traffico serve a stabilire un collegamento tra le misure di

cui all'articolo 16 e all'articolo 17 CCC. Per i dati di traffico, quest'ultima disposizione prevede alcune particolarità. Non sono contemplate le raccolte di dati informatici in tempo reale orientate al futuro né la conservazione dei dati, denominata «data retention». Queste sono disciplinate dagli articoli 20 e 21 CCC.

- 9 La conservazione può essere ordinata o effettuata in modo analogo.
 - a) Il termine «**ordinare**» comprende sia l'ordine giudiziario o amministrativo di conservare i dati sia l'obbligo di cooperazione attiva da parte del destinatario dell'ordine. Quest'ultima deve avvenire in modo tale che il destinatario dell'ordine conservi i dati inalterati e senza perdite (cfr. a questo proposito l'art. 16 cpv. 2 CCC).
 - b) La formulazione «**o in modo analogo**» consente agli Stati contraenti di organizzare la conservazione dei dati in modo flessibile e con i propri mezzi, in conformità al loro diritto procedurale.
- 10 Gli Stati contraenti dovrebbero stabilire misure di sicurezza in particolare quando vi è motivo di ritenere che i dati informatici siano particolarmente **suscettibili di perdita o alterazione**. Ciò può riferirsi, ad esempio, a situazioni in cui i dati sono soggetti a un breve periodo di conservazione in base alla politica aziendale, vengono cancellati a intervalli regolari o sono conservati in modo non sicuro.

B. Cpv. 2: Salvataggio dei dati mediante ordine di conservazione

- 11 L'art. 16 cpv. 2 CCC stabilisce che nei casi in cui i dati informatici sono protetti ai sensi dell'art. 16 cpv. 1 CCC mediante un ordine impartito a un'altra persona, gli Stati contraenti possono adottare misure e introdurre «**Preservation Orders**» per garantire l'integrità di tali dati informatici per un periodo di tempo limitato. Tuttavia, gli Stati contraenti non sono tenuti ad adottare tali misure. Gli Stati contraenti devono garantire che le loro autorità investigative possano ordinare o ottenere la conservazione immediata/tempestiva, indipendentemente dalla procedura scelta.
- 12 Sono **destinatari dell'ordine** le persone che sono in possesso di dati informatici memorizzati o che hanno il potere di disporne.
- 13 Gli Stati contraenti possono, nel diritto interno, come misura ai sensi dell'art. 16 cpv. 2 CCC, obbligare i destinatari dell'ordine a conservare, per tutto il

tempo necessario, ma al massimo per 90 giorni, l'integrità dei dati informatici oggetto dell'ordine. Possono tuttavia prevedere una proroga di tale **termine di conservazione**. La fissazione di un termine come misura serve a garantire alle autorità competenti il tempo necessario per ottenere le autorizzazioni richieste e avviare procedimenti legali quali perquisizioni, sequestri, confische o l'emissione di un ordine di consegna, affinché possano successivamente, in una seconda fase, prendere conoscenza del contenuto dei dati, in particolare anche nell'ambito dell'assistenza giudiziaria ai sensi dell'articolo 29 CCC.

C. Cpv. 3: Obbligo di segretezza

L'art. 16 cpv. 3 CCC impone agli Stati contraenti di adottare le misure legislative necessarie affinché, in caso di ordine rivolto al **depositario o a un terzo**, questi ultimi siano tenuti, per un periodo determinato dal diritto interno, a garantire la riservatezza delle operazioni di conservazione dei dati. Questa misura tiene conto, da un lato, dell'esigenza delle autorità di perseguimento penale di impedire che i sospetti e i terzi vengano a conoscenza delle indagini e, dall'altro, tutela la sfera privata delle persone interessate, in particolare di quelle menzionate nei dati o che possono essere identificate. 14

D. Cpv. 4

Con i **riferimenti** all'art. 16 cpv. 4 CCC, gli Stati contraenti si impegnano a garantire che i poteri e le procedure di cui all'art. 16 CCC siano soggetti alle condizioni e alle garanzie stabilite agli art. 14 e 15 CCC. 15

III. ATTUAZIONE IN SVIZZERA

La protezione dei dati informatici memorizzati ai sensi dell'articolo 16 CCC costituisce un importante **strumento investigativo** per la lotta contro i reati informatici e informatici. Gli Stati contraenti, compresa la Svizzera, sono tenuti a creare le condizioni quadro legislative e organizzative necessarie a tal fine. 16

La Svizzera non ha inserito nella vigente procedura penale svizzera la «procedura di congelamento rapido» prevista dall'articolo 16 CCC come misura autonoma. Il **diritto svizzero** rispetta invece in generale le disposizioni dell'art. 16 CCC, in quanto i **fornitori di servizi di** 17

telecomunicazione sono tenuti, da un lato, **ai sensi dell'art. 21 cpv. 2 e dell'art. 22 cpv. 2 LSCPT**, a garantire che al momento dell'instaurazione del rapporto con il cliente vengano raccolti i dati identificativi e che questi rimangano accessibili per tutta la durata del rapporto e per sei mesi dopo la sua cessazione e, dall'altro, e, dall'altro, **ai sensi dell'articolo 26 cpv. 5 LSCPT**, di conservare i dati secondari per sei mesi.

- 18 Anche da un punto di vista specifico, il diritto svizzero vigente soddisfa i requisiti della disposizione della Convenzione di cui all'articolo 16 CCC. Secondo il codice di procedura penale svizzero, i dati informatici possono essere acquisiti mediante un ordine scritto del pubblico ministero nell'ambito di una perquisizione ai sensi dell'**articolo 246 segg. CPP** o essere inseriti nel fascicolo mediante un'ordinanza di produzione ai sensi dell'**articolo 265 CPP**. In Svizzera, la conservazione dei dati informatici memorizzati può essere suddivisa in due categorie: la conservazione da parte delle autorità di perseguimento penale e la richiesta di conservazione a persone private. Entrambe le misure possono essere adottate dalla polizia, senza mandato del pubblico ministero, in caso di pericolo imminente, garantendo così una conservazione accelerata e proporzionata dei dati informatici memorizzati.

A. Salvaguardia da parte delle autorità di perseguimento penale

- 19 In Svizzera, la salvaguardia temporanea di materiale informatico è disposta, ai sensi dell'art. 198 in combinato disposto con l'art. 241 cpv. 1 e **l'art. 246 CPP**, con un'ordinanza del pubblico ministero (o, se del caso, del tribunale competente) al fine di perquisire registrazioni. Questo ordine garantisce che i dati possano essere esaminati per quanto riguarda il loro contenuto o la loro natura, al fine di determinarne l'idoneità come prova e, se del caso, di sequestrarli. Tali perquisizioni e la conservazione dei dati sono ordinate nella prassi della polizia ai sensi dell'art. 312 CPP. La polizia procede quindi alla perquisizione secondo le istruzioni del pubblico ministero (o del tribunale competente) e sequestra il supporto dati o esegue una copia forense dei dati presenti sui supporti da perquisire (cosiddetta «copia speculare»). La copia garantisce che i dati vengano copiati su un supporto esterno e siano protetti da manipolazioni. In particolare nei procedimenti penali in materia economica, ciò garantisce che i dati ai sensi dell'art. 16 cpv. 1 CCC possano essere immediatamente messi in sicurezza. D'altra parte, ciò consente alle persone interessate dalla perquisizione di continuare a utilizzare i propri

dispositivi per proseguire la propria attività commerciale, nel rispetto del principio di proporzionalità, fintantoché i dispositivi non devono essere sequestrati ai sensi dell'art. 263 CPP in combinato disposto con l'art. 69 cpv. 1 CP.

Per garantire la **salvaguardia dei dati su server digitali o nel cloud**, è ²⁰ assolutamente necessario effettuare immediatamente una copia dei dati in loco, al fine di impedire che questi dati vengano modificati o cancellati tramite vie di accesso alternative. La base giuridica per la realizzazione di copie di tali registrazioni e dati nell'ambito di una perquisizione è costituita dall'art. 247 cpv. 3 CPP.

B. Richiesta di conservazione a persone

Per quanto riguarda la perquisizione e il sequestro di materiale informatico, il ²¹ pubblico ministero (e, se del caso, anche il tribunale competente) ha inoltre la possibilità, ai sensi degli articoli 263 e 265 CPP, di ordinare con decisione la consegna e il sequestro di dati, ovvero di obbligare concretamente il detentore, sotto pena delle sanzioni previste dall'art. 292 CP e fissando un termine, a consegnare i supporti elettronici e i dati in originale o in copia come mezzi di prova. Questa procedura è denominata «**edizione**» e «**editare**». L'ordine di tale consegna è tuttavia possibile solo se il detentore non è né la persona imputata né una persona con diritto di rifiuto di testimoniare o di non rispondere né un'impresa che potrebbe essere ritenuta responsabile penalmente o civilmente in caso di consegna (art. 265 cpv. 2 CPP). Un ulteriore presupposto per l'emanazione di un'ordinanza di edizione è che l'ordinanza sia diretta al titolare effettivo dei dati con domicilio in Svizzera, altrimenti deve essere seguita la via dell'assistenza giudiziaria internazionale in materia penale.

Se una persona è tenuta, ai sensi dell'articolo 2 LSCPT, a trasmettere i dati ²² accessori di cui dispone relativi a una persona sorvegliata, si applicano gli articoli 269 segg. CPP. Se sono soddisfatti i presupposti di cui all'art. 269 cpv. 1 lett. b e c CPP e sussiste l'autorizzazione del tribunale delle misure di coercizione, non è possibile procedere a un sequestro ai sensi dell'art. 263 CPP, tuttavia i **fornitori di servizi di telecomunicazione** con sede in Svizzera, in qualità di titolari dei dati accessori, possono essere tenuti a effettuare una copia di sicurezza dei dati ai sensi dell'art. 273 CPP.

L'acquisizione di dati di inventario non costituisce una misura di coercizione e non richiede l'autorizzazione del tribunale delle misure di coercizione.

C. Mancanza di disposizioni legislative in materia di ordine di conservazione

- 23 In Svizzera, solo i fornitori di servizi di telecomunicazione sono tenuti per legge, ai sensi dell'articolo 2 LSCPT, a conservare i dati identificativi e i dati accessori per un periodo di sei mesi. In relazione a questi dati conservati, diverse autorità federali e cantonali hanno il diritto, ai sensi dell'**art. 15 LTC**, di ottenere informazioni sui servizi di telecomunicazione ai sensi dell'art. 21 LTC e sull'identificazione degli autori di reati ai sensi dell'art. 22 LTC. Tale comunicazione di informazioni è equiparabile a un obbligo di consegna ai sensi dell'art. 265 CPP. Non si tratta di un «preservation order» ai sensi dell'art. 16 cpv. 2 CCC.
- 24 Ratificando la Convenzione sulla criminalità informatica, la Svizzera non si è impegnata a introdurre i «preservation order» nel diritto interno. Attualmente, il codice di procedura penale svizzero non offre **alcuna base giuridica** per obbligare i titolari dei dati e i fornitori di servizi a proteggere i dati dalla perdita o dalla modifica e a tenerli a disposizione delle autorità di perseguimento penale senza doverli consegnare immediatamente. Il messaggio parte dal presupposto che la possibilità di obbligare chiunque a conservare dati mediante una decisione sarebbe eccessiva e difficilmente compatibile con il principio di proporzionalità. Questa valutazione non è più attuale: grazie alla digitalizzazione in continua evoluzione, oggi anche i privati dispongono di notevoli capacità di archiviazione sui propri supporti dati. Numerose aziende affidabili e disposte a collaborare dispongono volontariamente e in conformità con le disposizioni svizzere sulla protezione dei dati (LPD) di dati rilevanti a fini probatori, come ad esempio dati dei clienti e dati tecnici (non soggetti alla LSCPT), senza essere vincolate a un termine di conservazione. L'obbligo per i titolari di tali dati di prorogare il termine di conservazione al massimo di 90 giorni costituisce una misura molto più blanda rispetto all'ordine di perquisire i registri presso i titolari dei dati (cfr. supra N. 19 seg.) o di obbligarli a consegnare immediatamente tutti i dati (cfr. supra N. 21 seg.). In caso di proroga del termine di conservazione, i destinatari della decisione non sono soggetti a un onere sproporzionato, date le possibilità tecniche attualmente disponibili, e sussiste un interesse pubblico

a garantire che i dati raccolti volontariamente da privati possano essere conservati come prove ai fini dell'accertamento della verità prima di essere cancellati.

Ai sensi dell'attuale codice di procedura penale svizzero, la conservazione dei dati in possesso di persone che non rientrano nell'ambito di applicazione della LSCPT può essere garantita, in base al principio giuridico **argumentum a maiore ad minus**, anche mediante una decisione graduale: Può essere emanata una decisione ai sensi dell'art. 263 segg. CPP, con la quale il detentore dei dati è inizialmente obbligato, sotto minaccia della pena per disobbedienza ai sensi dell'art. 292 CP, a fornire informazioni, conservare i dati e mantenerne il segreto, al fine di raccogliere in una seconda fase i dati rilevanti per l'indagine e di trasmetterli agli atti d'indagine. Un tale obbligo graduale non è in contrasto con il principio del *numerus clausus* in materia di misure coercitive (art. 197 cpv. 1 lett. a CPP), poiché già il primo obbligo di conservazione dei dati ha lo scopo di richiedere successivamente i dati rilevanti ai fini probatori ai sensi dell'art. 263 CPP. Un obbligo graduale di questo tipo interferisce meno con i diritti del titolare dei dati rispetto all'ordine di perquisizione ai sensi degli articoli 246 segg. CPP o a un ordine di produzione di prove ai sensi dell'articolo 265 CPP. Il termine di conservazione massimo di 90 giorni previsto dall'art. 16 cpv. 2 CCC deve essere rispettato affinché la misura non vada oltre il testo della convenzione. 25

D. Blocco della conservazione da parte del Tribunale federale in caso di richiesta di sigillatura valida

Negli ultimi anni il Tribunale federale ha dovuto pronunciarsi più volte sulla situazione in cui, dopo il sequestro di apparecchi elettronici nonostante la sigillatura, le autorità inchiesta o un servizio specializzato incaricato hanno effettuato una copia di sicurezza forense (copia speculare) dei dati in essi contenuti. Il Tribunale federale ritiene inammissibile che, dopo una richiesta di sigillatura, un'autorità inchiesta disponga la duplicazione dei dati o la trasferisca a una persona o autorità da essa incaricata e vincolata alle sue istruzioni. L'autorità inquirente deve invece, dopo aver sigillato i supporti dati, presentare una richiesta di duplicazione al **tribunale delle misure coercitive, anche se la duplicazione è urgentemente necessaria per proteggere i dati dalla perdita**. La richiesta può essere presentata insieme alla domanda di rimozione del sigillo o, in caso di urgenza, con effetto 26

superprovvisorio. Dopo la sigillatura, l'ordine di duplicazione spetta esclusivamente al tribunale delle misure coercitive.

- 27 Questa giurisprudenza è stata giustamente oggetto di **critiche**. Essa risulta inoltre contraria al diritto internazionale alla luce della Convenzione sulla criminalità informatica. Il Tribunale federale ignora infatti che la Svizzera si è impegnata a garantire, nei procedimenti interni, la conservazione immediata dei dati informatici rilevanti ai fini della prova, al fine di evitare la perdita di prove. Con la sua giurisprudenza, il Tribunale federale introduce non solo una procedura superprovvisoria finora sconosciuta dinanzi al tribunale delle misure coercitive, ma anche una procedura in cui, anche in caso di ordinanza del giudice delle misure coercitive, l'acquisizione di dati rilevanti ai fini probatori può essere compromessa in modo significativo nel giro di poche ore: finché l'autorità inchiesta non può effettuare o far effettuare una copia dei dati durante una perquisizione in loco e deve invece rivolgersi al tribunale delle misure coercitive e attendere la sua decisione, nella prassi attuale non è possibile scongiurare il rischio considerevole che le persone autorizzate ad accedere ai dati conservati nei server digitali o nei cloud possano modificarli o cancellarli prima che il tribunale delle misure coercitive abbia deciso in merito alla copia. . I nuovi sviluppi offrono anche una maggiore protezione dall'accesso delle autorità, a meno che non si reagisca immediatamente. Recentemente, una delle più grandi aziende tecnologiche ha introdotto sui propri dispositivi (mobili) una funzione di sicurezza che blocca la porta USB 60 minuti dopo l'ultimo sblocco del dispositivo, con la conseguenza che da quel momento in poi non è più possibile leggere i dati né installare sul dispositivo un software che ne consenta la lettura successiva. È presumibile che altre aziende seguiranno questo esempio. Di conseguenza, determinate situazioni di pericolo – sia nuove che quelle prese in considerazione nella relazione esplicativa – possono essere evitate solo con l'intervento immediato dell'autorità inquirente, ovvero della polizia o della persona incaricata da quest'ultima durante la perquisizione in loco. La procedura stabilita dal Tribunale federale, che prevede la presentazione di una richiesta di mirroring superprovvisorio al tribunale delle misure coercitive dopo la sigillatura, aumenta notevolmente il rischio di perdita di prove. Non si può quindi parlare di un'efficace perseguimento penale ai sensi della Convenzione sulla criminalità informatica.

BIBLIOGRAFIA

Burgermeister Daniel, Beweiserhebung in der Cloud, Master of Advanced Studies in Forensics (MAS Forensics), August 2015.

Graf Damian K., Praxishandbuch zur Siegelung, StPO inklusive revidierter Bestimmungen – VStrR – IRSG – MStP, Bern 2022.

Graf Damian K./Günal Rütsche Serdar, Datensicherung von Mobiltelefonen und Tablets – technische und (siegelungs-)rechtliche Herausforderungen im Strafverfahren, SJZ 121 (2025), S. 604 ff.

Hansjakob Thomas, Überwachungsrecht der Schweiz, Kommentar zu Art. 269 ff. StPO und zum BÜPF, Zürich 2018.

I MATERIALI

Bundesamt für Justiz, Vernehmlassungsentwurf, Genehmigung und Umsetzung des Übereinkommens des Europarates über die Cyberkriminalität, Vorentwurf und Erläuternder Bericht, Bern, März 2009, abrufbar unter <https://www.bj.admin.ch/bj/de/home/sicherheit/gesetzgebung/archiv/cybercrime-europarat.html>, besucht am 4.5.2025.

Botschaft über die Genehmigung und die Umsetzung des Übereinkommens des Europarates über die Cyberkriminalität vom 18.6.2010, BBl 2010 4697 ff., abrufbar unter <https://www.fedlex.admin.ch/eli/fga/2010/813/de>, besucht am 4.5.2025.

Botschaft zur Änderung des Schweizerischen Strafgesetzbuches (Allgemeine Bestimmungen, Einführung und Anwendung des Gesetzes) und des Militärstrafgesetzes sowie zu einem Bundesgesetz über das Jugendstrafrecht vom 21.9.1998, BBl 1999 II 1799 ff., abrufbar unter https://www.fedlex.admin.ch/eli/fga/1999/1_1799_1787_1669/de, besucht am 4.5.2025.

Europarat, Explanatory Report to the Convention on Cybercrime, Budapest, 23.11.2001, abrufbar unter <https://rm.coe.int/16800cce5b>, besucht am 4.5.2025 (zit. Explanatory Report).

Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung

personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), abrufbar unter <https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX%3A32016R0679>, besucht am 4.5.2025.

ATTENZIONE: Questa versione del commentario è una traduzione automatica dell'originale. Il commentario originale è in tedesco. La traduzione è stata effettuata con www.deepl.com. Solo la versione originale fa fede. La forma tradotta del commentario non può essere citata

COMMENTO SU

Art. 18 CCC (Convenzione sulla cybercriminalità [Cybercrime Convention])

Un commentario di Damian K. Graf

CITAZIONE SUGGERITA

Damian K. Graf, Commentario all'art. 18 CCC, in: Damian K. Graf (a cura di), Commentario online alla Convenzione sulla cybercriminalità [Cybercrime Convention]

Breve citazione: OK-Graf, art. 18 CCC N. XXX.

Titolo 3: Ingiunzione di produrre dati

Art. 18 Ingiunzione di produrre dati

¹ Le Parti adottano le misure legislative e di altra natura necessarie per consentire alle autorità competenti di ordinare:

a. a un soggetto sul loro territorio di fornire specifici dati informatici in suo possesso o sotto il suo controllo, memorizzati in un sistema informatico o su un supporto di salvataggio di dati informatici; e

b. a un fornitore di servizi che offre le proprie prestazioni sul loro territorio di fornire i dati in suo possesso o sotto il suo controllo relativi agli utenti e a tali servizi.

² Le facoltà e le procedure di cui al presente articolo sono subordinate agli articoli 14 e 15.

³ Ai sensi del presente articolo, l'espressione «informazioni relative agli utenti» designa ogni informazione detenuta sotto forma di dati informatici o sotto altra forma da un fornitore di servizi e riguardante gli utenti dei suoi servizi, fatta eccezione per i dati relativi al traffico informatico o al contenuto, e che permette di stabilire:

a. il tipo di servizio di comunicazione utilizzato, le misure tecniche adottate a tal fine e la durata del servizio;

b. l'identità dell'utente, il suo indirizzo postale o geografico, il suo numero di telefono e gli altri numeri d'accesso e i dati riguardanti la fatturazione e il pagamento disponibili in base al contratto o all'accordo di fornitura del servizio;

c. ogni altra informazione sul luogo di installazione dell'apparecchiatura di comunicazione, disponibile in base al contratto o all'accordo di fornitura del servizio.

STRUTTURA

I. Considerazioni generali.....	166
II. Ordine di consegna di dati informatici (cpv. 1 lett. a).....	167
III. Ordine di consegna di dati di inventario ai provider (cpv. 1 lett. b)	170
IV. Rinvio agli articoli 14–15 CCC (cpv. 2)	173
V. Definizione dei dati di inventario (cpv. 3).....	174
VI. Presupposti per la liceità della raccolta dei dati secondo il diritto processuale penale svizzero	175
Bibliografia	177
I materiali.....	178

I. CONSIDERAZIONI GENERALI

- 1 Nella sezione 2 («Diritto procedurale») del capitolo 2 («Misure da adottare a livello interno»), l'articolo 18 CCC, al titolo 3 («Ordinanza di consegna»), disciplina la **consegna di dati** da parte delle autorità penali competenti. Si distinguono due casi: da un lato, la consegna di dati informatici da parte di una persona che si trova nel territorio dello Stato contraente interessato (cpv. 1 lett. a), dall'altro, la divulgazione di dati di inventario da parte di fornitori di servizi che offrono i loro servizi nello Stato contraente (cpv. 1 lett. b). Poiché questi ultimi non hanno sede nello Stato contraente interessato e i dati di inventario non devono necessariamente essere memorizzati in tale Stato, l'art. 18 CCC contiene un elemento **extraterritoriale** (cfr. n. 9 segg.).
- 2 L'emanazione di un'ordinanza di consegna dei dati costituisce il **mezzo meno severo** rispetto alle misure coercitive che interferiscono in modo più profondo con i diritti delle persone interessate (spesso non accusate). In conformità con il principio di proporzionalità, la possibilità di un'ordinanza di divulgazione deve sempre essere esaminata prima di ricorrere a misure coercitive di più ampia portata (come ad esempio una perquisizione domiciliare) (cfr. anche art. 265 cpv. 4 CPP). Un aspetto essenziale nella ponderazione degli interessi è il rischio di collusione e di perdita di prove se i dati non vengono immediatamente sequestrati dai membri delle autorità di perseguimento penale.
- 3 Dal punto di vista del contenuto, l'articolo 18 CCC è limitato alla consegna di dati **concretamente determinati o determinabili, già esistenti o memorizzati nell'ambito di un procedimento penale**. Non è necessario che si tratti di un reato informatico ai sensi degli articoli 2–11 CCC o di un altro reato commesso con un sistema informatico; è sufficiente che le prove disponibili in forma elettronica servano a provare un reato qualsiasi (art. 14 cpv. 2 CCC). Ciò significa anche che il materiale probatorio richiesto deve essere almeno **potenzialmente rilevante**, ossia può essere importante per l'indagine penale o non deve apparire manifestamente inidoneo, come risulta già dal principio generale di proporzionalità (presupposto di una misura statale «adeguata»).
- 4 In base al testo della Convenzione («ciascuna Parte contraente adotta le misure legislative o di altra natura necessarie per autorizzare le proprie

autorità competenti»; analogamente anche art. 14 cpv. 1 CCC), l'art. 18 CCC **non è una norma «autoesecutiva»** che trova applicazione diretta con la ratifica della Convenzione. Essa costituisce piuttosto un obbligo di diritto internazionale che impone l'adozione di norme interne corrispondenti. L'art. 18 CCC non può quindi, contrariamente all'art. 32 CCC, essere invocato direttamente come base per una misura di procedura penale.

Tuttavia, nel messaggio il Consiglio federale ha dichiarato che **il diritto svizzero soddisfa già i requisiti dell'art. 18 CCC**. In tal senso, sia il testo dell'art. 18 CCC che i relativi materiali – in particolare la relazione esplicativa alla CCC e la Guidance Note # 10 del Cybercrime Convention Committee («T-CY») del Consiglio d'Europa – possono essere utilizzati come **ausili interpretativi** per l'applicazione delle disposizioni nazionali, in primo luogo l'art. 265 CPP. In Svizzera, inoltre, è un principio generale che le norme devono essere interpretate, per quanto possibile, in conformità con le convenzioni.

L'art. 18 CCC non stabilisce come le misure debbano essere attuate esattamente nel diritto interno, ma si limita a delineare il contenuto minimo delle norme nazionali in materia di competenza e lascia ai singoli Stati contraenti il compito di integrare le disposizioni della convenzione nel loro sistema di misure di assunzione delle prove. L'art. 18 cpv. 2 CCC rinvia comunque alle ulteriori garanzie minime degli art. 14–15 CCC, che devono essere rispettate anche in questo contesto.

L'art. 18 CCC non disciplina nemmeno se e, in caso affermativo, in quale misura i dati debbano essere conservati, né stabilisce termini di conservazione. In particolare, non contiene alcun obbligo per i fornitori di servizi di conservare registrazioni sui propri abbonati, di garantirne l'esattezza, di verificare l'identità degli utenti o di impedire l'uso di pseudonimi. Tali obblighi possono eventualmente derivare da norme interne a livello di legge o di ordinanza.

II. ORDINE DI CONSEGNA DI DATI INFORMATICI (CPV. 1 LETT. A)

Dal punto di vista oggettivo, la richiesta di consegna può estendersi ai «dati informatici», definiti all'art. 1 lett. b CCC come «qualsiasi rappresentazione di fatti, informazioni o concetti in una forma adatta al trattamento in un sistema

informatico, compreso un programma che può far eseguire una funzione da un sistema informatico». Questo concetto comprende **tutti i tipi di dati**, in particolare i dati di inventario, di collegamento e di contenuto (cfr. n. 24 segg.). L'art. 18 CCC richiede solo che i dati in questione possano essere richiesti, senza tuttavia pronunciarsi sulla competenza o sulla procedura specifica prevista dall'ordinamento interno. Per questo motivo, ad esempio, è perfettamente compatibile con gli articoli 18 e 15 CCC che la consegna di dati di connessione sia soggetta, secondo il diritto svizzero, a requisiti più severi rispetto alla consegna di dati di inventario o di contenuto e che sia inoltre necessaria l'autorizzazione del tribunale competente in materia di misure coercitive (cfr. n. 27 segg.).

- 9 **Dal punto di vista personale**, l'art. 18 cpv. 1 lett. a CCC si applica, secondo il suo testo esplicito, a tutte le persone giuridiche e fisiche che, al momento dell'ordinanza, hanno la loro sede, il loro domicilio o anche solo la loro dimora provvisoria nello Stato contraente. Il rapporto interno richiesto dal diritto sovranitario non è definito in questo caso – contrariamente all'art. 32 CCC, non è definito in base al luogo di memorizzazione dei dati, ma è **collegato alla persona in possesso o sotto il controllo della quale si trovano i dati da raccogliere**. L'art. 18 cpv. 1 lett. a CCC comprende anche i **provider** con sede in Svizzera; da questi possono essere resi disponibili non solo i dati di inventario (cfr. art. 18 cpv. 1 lett. b CCC), ma anche i dati relativi al contenuto e alla connessione.
- 10 Il luogo di memorizzazione dei dati è irrilevante in questo contesto. Di conseguenza, anche **i dati memorizzati all'estero** possono essere consultati presso una persona residente in Svizzera, a condizione che tali dati siano «in suo possesso o sotto il suo controllo» («computer data in that person's possession or control»). L'art. 18 cpv. 1 lett. a CCC consente quindi, come l'art. 32 CCC, una forma di acquisizione extraterritoriale delle prove. Ciò è in linea con la giurisprudenza del Tribunale federale relativa all'art. 18 CCC e all'art. 265 CPP, secondo cui tali disposizioni **consentono l'edizione di tutti i dati a cui il destinatario della decisione può o è autorizzato ad accedere** («avoir un pouvoir de disposition, en fait et en droit, sur ces données»).
- 11 La coppia di concetti «possesso o controllo» si riferisce, da un lato, al **possesso fisico** dei dati in questione nel territorio dello Stato contraente che ha emesso la decisione (dominio sui dati) e, dall'altro, a situazioni in cui i dati di interesse non si trovano nella sfera di custodia del destinatario della

decisione di divulgazione, ma quest'ultimo può **liberamente controllarne** la consegna (diritto di disposizione). Ciò comprende, ad esempio, una persona che ha memorizzato dati presso un fornitore terzo, ad esempio in un cloud: in questo caso il fornitore terzo è in possesso dei dati e l'utente ne ha il controllo, ed entrambi possono essere chiamati individualmente a rispondere in qualità di destinatari della disposizione. Possesso e controllo possono quindi divergere. Secondo la relazione esplicativa, tuttavia, non è sufficiente disporre della sola capacità tecnica di accedere a dati memorizzati a distanza; i dati devono piuttosto essere sotto il controllo legittimo («legitimate control») del destinatario della disposizione. Il «controllo» presuppone quindi cumulativamente la possibilità di accedere a tali dati e l'autorizzazione ad accedervi. Ciò deve essere chiarito nel dettaglio. Il destinatario del trattamento deve **collaborare** alla dimostrazione se fa valere la mancanza di controllo o di accesso alle informazioni richieste.

Nelle **strutture di gruppo**, non si può dare per scontato che una società 12 controllata possa accedere ai dati della società madre o delle società affiliate. Viceversa, le società capogruppo, in virtù della loro posizione, dovrebbero spesso disporre o controllare i dati all'interno del gruppo, sia di fatto che di diritto. Se i dati rimangono presso le società nazionali per motivi normativi o di protezione dei dati e la società madre non ha dimostrabilmente accesso ad essi, i dati possono essere richiesti solo alla società nazionale. Se vengono utilizzate soluzioni di archiviazione o di conservazione interne o esterne all'azienda o centri di dati, il diritto di controllo rimane alla persona che ha esternalizzato il servizio, mentre l'azienda che conserva i dati ne è «proprietaria», poiché questi si trovano nella sua sfera di controllo. Pertanto, anche le società affiliate o partner di fornitori stranieri con sede in Svizzera che memorizzano dati in Svizzera (ad es. in server farm) sono soggette all'obbligo di consegna.

È determinante la possibilità di accesso effettiva o giuridica **al momento 13 dell'ordine**. Limitare l'accesso dopo aver ricevuto una richiesta non solo costituirebbe un abuso di diritto, ma potrebbe anche configurare un reato a seconda della situazione giuridica degli Stati contraenti (cfr. art. 305 CP [favoreggiamento]).

Come visto (n. 9 segg.), l'art. 18 cpv. 1 lett. a CCC non si riferisce direttamente 14 al luogo di memorizzazione dei dati. Una decisione di consegna emessa in Svizzera può tuttavia riguardare dati memorizzati in Svizzera

indipendentemente dal fatto che le persone aventi diritto ai dati si trovino all'estero (ad esempio se una persona domiciliata all'estero memorizza dati in Svizzera o gestisce un centro dati). Se solo i dati si trovano in Svizzera, ma non le persone aventi diritto ai dati, si pone solo la questione di come la richiesta di consegna possa essere trasmessa alla persona domiciliata all'estero – una questione che diventa attuale anche alla lett. b (cfr. n. 20 seg.).

III. ORDINE DI CONSEGNA DI DATI DI INVENTARIO AI PROVIDER (CPV. 1 LETT. B)

- 15 L'art. 18 cpv. 1 lett. b CCC si riferisce alla consegna di **dati di inventario** da parte di **fornitori di servizi o «service provider»** ai sensi dell'art. 1 lett. c CCC che offrono i loro **servizi nel territorio dello Stato contraente**. L'articolo ha quindi una portata sia più restrittiva che più ampia rispetto alla lett. a, in quanto da un lato si limita ai fornitori di servizi e alla presentazione di dati relativi agli abbonati («subscriber information») – ad esempio l'identità del cliente o informazioni relative alle operazioni di pagamento (cfr. n. 24 segg.) – e dall'altro non riguarda solo i fornitori svizzeri, ma anche quelli stranieri (cfr. al riguardo n. 17 segg.). Il necessario rapporto interno con la Svizzera è inteso qui, analogamente alla concezione del diritto antitrust, nel senso del **principio di effetto**, motivo per cui sono contemplati anche i fornitori di servizi stranieri se attivi sul mercato svizzero. Anche in questo caso rimane il presupposto che i dati siano **in possesso o sotto il controllo** del destinatario della disposizione (cfr. al riguardo n. 11 segg.).
- 16 Contrariamente all'art. 32 CCC, che si basa sulla volontarietà e presuppone, tra l'altro, un'autorizzazione nelle condizioni generali di contratto o simili per una consegna dei dati conforme alla legge da parte dei fornitori, una richiesta di consegna è **vincolante** e deve essere eseguita dai fornitori di servizi destinatari, purché sia conforme ai requisiti interni dello Stato contraente in cui sono offerti i servizi e che ha emesso la decisione. L'accesso facilitato ed efficiente ai dati di inventario appare opportuno, poiché l'80-90 % dei dati richiesti a livello internazionale sono dati di inventario; l'art. 18 cpv. 1 lett. b CCC contribuisce quindi ad alleggerire il sistema di assistenza giudiziaria internazionale.
- 17 Per quanto riguarda la questione di quando un servizio è «offerto» **in uno Stato contraente**, negli Stati europei esiste già una giurisprudenza in altri

contesti: è necessario che le attività del fornitore di servizi siano rivolte agli utenti dello Stato, ovvero che il fornitore di servizi intenda che gli utenti di tale Stato utilizzino i suoi servizi. La semplice accessibilità di un sito web o la possibilità di registrarsi da un altro Paese non è sufficiente a tal fine. Indizi dell'«offerta» di un servizio possono essere, ad esempio, l'uso di lingue o valute diverse da quelle usuali nello Stato di sede, l'uso di domini di primo livello o di un prefisso telefonico di uno Stato. Ad esempio, la Corte suprema belga ha stabilito che Yahoo! Inc. poteva essere obbligata, sotto pena di sanzioni penali, a consegnare i dati relativi ai propri utenti perché, in qualità di fornitore di un servizio di webmail gratuito, partecipava attivamente alla vita economica belga. Ciò è emerso, tra l'altro, dall'uso del dominio «www.yahoo.be», dall'uso della lingua nazionale, dalla pubblicità basata sulla localizzazione degli utenti e dalla creazione di un modulo di reclamo e di una sezione FAQ per gli utenti belgi. Infine, il nuovo art. 3, n. 4, del regolamento (UE) 2023/1543 relativo agli ordini europei di consegna di prove e agli ordini europei di conservazione di prove elettroniche nei procedimenti penali e all'esecuzione di pene detentive a seguito di procedimenti penali del 12 luglio 2023 («regolamento e-evidence») richiede che il criterio della «prestazione di servizi nell'UE» sia cumulativo (a) la creazione di una possibilità per le persone fisiche o giuridiche in uno Stato membro di usufruire dei servizi e (b) un legame sostanziale con tale Stato membro, che si considera sussistere, ad esempio, quando il fornitore di servizi ha una sede o un numero significativo di utenti in tale Stato membro o in più Stati membri o quando la sua attività è orientata verso di essi. Tali criteri possono essere utilizzati anche per l'articolo 18 CCC.

Se i fornitori stranieri sono attivi con un servizio nel mercato di uno Stato 18
contraente, sono tenuti a comunicare i dati di inventario relativi agli utenti di tale servizio specifico nello Stato contraente in questione. È il caso, ad esempio, di chi si registra tramite l'indirizzo «.ch» del fornitore di servizi, ha indicato la Svizzera come suo domicilio o sede o ha utilizzato un indirizzo IP svizzero al momento della registrazione o in un momento successivo.

Anche all'interno degli organi del Consiglio d'Europa prevale l'opinione che 19
sia possibile richiedere a un **provider nazionale** i dati di inventario **memorizzati all'estero** su un sistema di elaborazione dati (purché siano sotto il suo controllo, cfr. anche n. 11 segg.) e che le ordinanze possano essere

indirizzate direttamente a un **provider estero**. Entrambe le posizioni sono in linea con il testo dell'articolo 18 CCC.

- 20 Anche il Tribunale federale si è già pronunciato su queste due questioni, formulando un giudizio differenziato: In una sentenza del 16 novembre 2016 ha stabilito che l'art. 18 CCC e l'art. 265 CPP consentono la produzione di tutti i dati, purché il destinatario della decisione possa effettivamente e legalmente accedervi («avoir un pouvoir de disposition, en fait et en droit, sur ces données»), quindi anche quelli conservati all'estero. Con sentenza del 14 gennaio 2015 ha invece dichiarato che, sulla base dell'art. 18 CCC, non è possibile rivolgersi direttamente a un provider straniero mediante un'ordinanza di produzione, anche se questi offre i propri servizi in Svizzera – l'art. 32 CCC disciplina quindi in modo esaustivo l'accesso transfrontaliero diretto e l'art. 25 cpv. 4, prima frase, CCC stabilisce che l'assistenza giudiziaria internazionale deve seguire gli strumenti usuali, a meno che la CCC non preveda «espressamente» una disposizione diversa. Il Tribunale federale ha comunque constatato che le filiali o le società partner di provider stranieri con sede in Svizzera che memorizzano dati in Svizzera (come ad esempio le server farm) sono soggette al diritto svizzero. Tuttavia, non ha esaminato né il testo dell'articolo 18 CCC né la relazione esplicativa o il messaggio, secondo cui il legislatore partiva proprio dal presupposto che il diritto interno fosse conforme ai requisiti dell'articolo 18 CCC. Non spetta al Tribunale federale prevalere sulla chiara volontà del legislatore. Inoltre, non si ravvisa alcuna violazione della sovranità quando i servizi sono offerti in Svizzera, poiché in questo caso sussiste proprio un sufficiente legame interno con la Svizzera. Una limitazione ai fornitori di servizi con sede in Svizzera renderebbe obsoleto l'art. 18 cpv. 1 lett. b CCC, poiché i provider con sede in Svizzera sono già contemplati dall'art. 18 cpv. 1 lett. a CCC (cfr. n. 9) e devono quindi fornire non solo i dati relativi all'esistenza, ma anche quelli relativi al contenuto e alla connessione. Pertanto, a ben vedere, anche l'art. 18 cpv. 1 lett. b CCC può essere utilizzato come base per la prassi corrente in Svizzera, che si fonda principalmente sull'art. 32 CCC, secondo cui le autorità di perseguimento penale rivolgono **richieste dirette ai provider stranieri** («richieste di informazioni»). Ciò vale anche in senso inverso: i provider svizzeri che offrono i loro servizi sui mercati esteri possono essere invitati direttamente dalle autorità di quei paesi a consegnare i dati e, poiché sono fondamentalmente soggetti all'obbligo di consegna, non sono punibili ai sensi

dell'articolo 271 CP («Atto proibito a favore di uno Stato straniero») in caso di consegna dei dati.

Per quanto riguarda la **notifica** delle decisioni di divulgazione, i provider di grandi dimensioni mettono a disposizione i cosiddetti «portali di applicazione della legge», attraverso i quali anche le autorità di perseguimento penale svizzere possono registrarsi e inserire direttamente le loro richieste. Nel caso di fornitori di servizi più piccoli, le richieste di consegna possono essere trasmesse tramite la polizia (via Interpol) o, se accettato, anche direttamente (ad esempio via e-mail). L'art. 18 cpv. 1 lett. b CCC consente in tal senso di rinunciare alla via formale dell'assistenza giudiziaria e permette agli Stati contraenti di notificare tali decisioni di divulgazione direttamente ai provider di altri Stati contraenti. Ciò è ammissibile e opportuno, poiché l'obbligo di notificare la decisione di esibizione mediante assistenza giudiziaria vanificherebbe le agevolazioni che l'art. 18 cpv. 1 lett. b CCC intende proprio garantire. Solo la notifica diretta garantisce che le autorità di polizia possano accedere in modo efficiente e rapido ai dati necessari, senza dover ricorrere alla procedura di assistenza giudiziaria, spesso lunga e burocratica. È tuttavia un dato di fatto che la mancanza di cooperazione non può essere **imposta** direttamente, ma solo attraverso la procedura formale di assistenza giudiziaria mediante misure coercitive che vanno oltre l'art. 18 CCC. 21

Poiché la richiesta di consegna è una **misura interna di assunzione di prove**, non è determinante il diritto dello Stato contraente in cui ha sede il provider, bensì quello dello Stato contraente in cui il provider offre i propri servizi. 22

IV. RINVIO AGLI ARTICOLI 14–15 CCC (CPV. 2)

Nell'ambito dell'art. 15 CCC, gli Stati possono stabilire **condizioni e misure di salvaguardia** ed escludere dati dall'ambito di applicazione dell'art. 18 CCC. È giustificato, ad esempio, limitare la consegna dei dati relativi alle comunicazioni a determinati reati e richiedere a tal fine l'autorizzazione del tribunale competente a disporre misure coercitive (art. 273 CPP). È inoltre ammesso subordinare le decisioni di consegna a divieti di comunicazione, come previsto dal diritto svizzero (art. 73 cpv. 2 CPP). 23

V. DEFINIZIONE DEI DATI DI INVENTARIO (CPV. 3)

- 24 Sono considerati **dati di inventario** tutte le informazioni – che non sono qualificabili come dati di collegamento o di contenuto – memorizzate da un fornitore di servizi in relazione a un utente o a un abbonato dei suoi servizi. L'obiettivo principale della richiesta di dati di inventario è determinare l'**identità** dell'abbonato o dell'utente e individuare i servizi utilizzati dall'utente. Possono inoltre essere rilevanti anche informazioni commerciali quali dati di fatturazione e di pagamento, in particolare in relazione a frodi informatiche e altri reati contro il patrimonio.
- 25 Ai sensi dell'art. 18 cpv. 3 CCC, i dati di inventario comprendono tutte le informazioni relative (a) al tipo di servizio di comunicazione utilizzato, alle misure tecniche adottate a tal fine e alla durata del servizio; (b) all'identità dell'utente, il suo indirizzo postale o domiciliare, i numeri di telefono e altri numeri di accesso, nonché le informazioni relative alla fatturazione e al pagamento disponibili sulla base del contratto o dell'accordo relativo al servizio; nonché (c) altre informazioni relative all'ubicazione dell'impianto di comunicazione disponibili sulla base del contratto o dell'accordo relativo al servizio. In Svizzera, le informazioni che possono essere comunicate ai sensi dell'art. 22 cpv. 1 LSCPT sono concretizzate in particolare negli articoli 36-38 dell'ordinanza del 15 novembre 2017 concernente la sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni («OSCT», RS 780.11). Sono considerati dati di inventario in particolare gli elementi di indirizzamento quali l'assegnazione di nomi, numeri di telefono e indirizzi dell'utente a un indirizzo IP noto, nonché i contratti originali e le copie dei documenti d'identità presentati al momento della conclusione del contratto e le informazioni tecniche relative alle telecomunicazioni.
- 26 I dati di inventario devono essere distinti dai **dati di contenuto**, che comprendono il contenuto della comunicazione o i file memorizzati, nonché dai dati di connessione o **di traffico**, che sono generati in relazione a una comunicazione e dai quali è possibile determinare l'origine, la destinazione, l'itinerario, l'ora, la data, l'entità o la durata della comunicazione (art. 1 lett. d CCC). Il Tribunale federale distingue i dati di inventario dai dati marginali in base al criterio di demarcazione secondo cui, se le autorità di perseguimento penale sono già a conoscenza di un collegamento Internet o di un indirizzo e-mail che deve solo essere attribuito a una persona specifica, si tratta di una richiesta di dati di inventario. Se invece le autorità di perseguimento penale

sono a conoscenza solo di attività di comunicazione Internet punibili e gli indirizzi IP assegnati e i clienti registrati devono essere determinati solo tramite i dati marginali di connessione della comunicazione in questione, si tratta di una raccolta retroattiva (soggetta ad autorizzazione) di dati marginali ai sensi dell'art. 273 CPP. Secondo la giurisprudenza, ciò vale in linea di principio anche per la richiesta di consegna di una cronologia IP. Correttamente, la distinzione va operata a seconda che si tratti di stabilire chi ha comunicato con chi e quando (dati di connessione ai sensi dell'art. 273 CPP) o piuttosto chi ha utilizzato un determinato servizio in un momento noto (dati di inventario ai sensi dell'art. 22 cpv. 1 LSCPT). Gli indirizzi IP di registrazione per un account già noto devono quindi essere considerati chiaramente come dati di inventario e non come dati di traffico, poiché servono esclusivamente all'identificazione di un partecipante e non hanno alcun

riferimento alla successiva comunicazione tramite l'account. Anche altri «**access data**» (ad es. la cronologia IP degli accessi a un servizio non destinato alla comunicazione, come l'accesso a un portafoglio crittografico o a un cloud) non possono essere considerati dati marginali di connessione. Questi dati non riguardano né direttamente né indirettamente la comunicazione tra persone e la sua sorveglianza. In tali casi, gli indirizzi IP sono piuttosto paragonabili a tracce lasciate sulla scena del crimine, simili a un'impronta digitale o al DNA, e non costituiscono dati accessori nel contesto della comunicazione umana, ma piuttosto dati di inventario. La sentenza del Tribunale federale sulla qualificazione delle cronologie IP come dati di traffico ai sensi dell'art. 273 CPP è in tal senso troppo poco differenziata.

VI. PRESUPPOSTI PER LA LICEITÀ DELLA RACCOLTA DEI DATI SECONDO IL DIRITTO PROCESSUALE PENALE SVIZZERO

Per i **dati di inventario** ai sensi dell'art. 18 cpv. 3 CCC – ossia in particolare le indicazioni (anche retroattive) relative a chi è o era registrato come titolare o destinatario della fattura del collegamento presso i fornitori di servizi soggetti al diritto svizzero (cfr. n. 24 segg.) – può essere presentata una semplice richiesta ai sensi dell'art. 22 cpv. 1 LSCPT presso l'autorità di sorveglianza della corrispondenza postale e della telecomunicazione (servizio ÜPF). Tali informazioni possono essere ottenute anche mediante edizione 27

(art. 265 CPP), in particolare se il provider estero che offre i propri servizi ai sensi dell'art. 18 cpv. 1 lett. b CCC in Svizzera non è soggetto alla LSCPT. La richiesta di informazioni tramite il servizio PTIP costituisce solo una norma di procedura; né il CPP né la LSCPT o la relativa ordinanza prevedono che le informazioni non comunicate tramite il servizio PTIP siano inutilizzabili. Una richiesta di dati di inventario presuppone il sospetto che sia stato commesso un reato (delitto, contravvenzione o infrazione) tramite Internet (art. 22 cpv. 1 LSCPT), la potenziale rilevanza per l'indagine o l'ammissibilità come prova delle informazioni richieste, nonché la proporzionalità. Contro una consultazione di dati di inventario non è ammesso alcun ricorso ordinario; in particolare, la sigillatura (art. 248 CPP) non è pertinente, poiché non è riconoscibile a priori in che misura i dati di inventario richiesti potrebbero essere soggetti a un divieto di sequestro ai sensi dell'art. 264 CPP. I provider sono soggetti all'obbligo di fornire informazioni; se si rifiutano, può essere inflitta un'ammenda d'ordine o un'ammenda ai sensi dell'articolo 292 CP (purché ne siano stati informati in precedenza) oppure possono essere adottate misure coercitive (analogamente all'articolo 265 cpv. 3 e 4 CPP). Per i provider stranieri che offrono i loro servizi in Svizzera, la minaccia di una pena ai sensi dell'art. 292 CP dovrebbe essere ammessa, ma le misure coercitive per l'esecuzione della richiesta di dati relativi al traffico dovrebbero essere richieste allo Stato competente in via di assistenza giudiziaria.

- 28 Per i dati relativi al contenuto e alla connessione, che possono essere richiesti ai sensi dell'art. 18 cpv. 1 lett. a CPP, occorre poi operare una distinzione: **i dati relativi al contenuto** che possono essere rilevanti ai fini probatori devono essere consegnati ai sensi dell'art. 265 CPP, purché siano memorizzati («in storage») al momento dell'ordinanza e non si trovino ancora in fase di trasmissione («in traffic»). Di rilevanza pratica sono ad esempio i dati relativi al contenuto dei gestori di webmail, come l'account di posta elettronica di un indirizzo «@bluewin.ch» presso Swisscom. Il presupposto per la consegna dei dati relativi al contenuto è un sospetto fondato di un reato qualsiasi, la potenziale rilevanza probatoria o la possibile rilevanza delle registrazioni consegnate per il procedimento penale, nonché il rispetto del principio di proporzionalità. La decisione di divulgazione può essere accompagnata da un divieto di comunicazione ai sensi dell'art. 73 cpv. 2 CPP, il che significa che il gestore del servizio non può informare il titolare dell'account fino a nuovo ordine. Contro un'ordinanza di produzione è possibile ricorrere alla sigillatura (art. 248 CPP) da parte dei titolari e delle altre persone aventi diritto, sempre

che possano far valere propri interessi al segreto. Il provider ha formalmente il diritto alla sigillatura, ma non può richiederla in vece dei propri clienti e difficilmente potrà mai far valere propri divieti di sequestro ai sensi dell'art. 264 CPP. Per i **dati di collegamento o marginali** (cfr. n. 26), il pubblico ministero non deve disporre la produzione, bensì emanare un'ordinanza ai sensi dell'art. 273 CPP, soggetta a requisiti più severi: (1) deve sussistere un forte sospetto di un crimine o di un delitto; (2) la gravità del reato deve giustificare la sorveglianza; (3) gli atti d'indagine compiuti finora devono essere rimasti infruttuosi o le indagini sarebbero altrimenti senza prospettive o sarebbero rese eccessivamente difficili (art. 273 cpv. 1 in combinato disposto con l'art. 269 cpv. 1 CPP). L'ordinanza deve inoltre essere approvata dal tribunale delle misure di coercizione (art. 274 CPP), altrimenti le prove raccolte sono assolutamente inutilizzabili (art. 277 cpv. 2 CPP). L'approvazione del tribunale delle misure coercitive può essere impugnata dalla persona sorvegliata, eventualmente anche dal provider, con ricorso ai sensi dell'art. 393 segg. CPP (art. 279 cpv. 3 CPP).

BIBLIOGRAFIA

Betschmann Simon, Randdatenerhebung im Fernmeldeverkehr gemäss Art. 273 StPO, AJP 2019, S. 358 ff.

Donatsch Andreas/Lieber Viktor/Summers Sarah/Wohlers Wolfgang (Hrsg.), Schulthess Kommentar zur Schweizerischen Strafprozessordnung, 3. Aufl., Zürich 2020 (zit. SK-Bearbeiter/in, Art. ... StPO N. ...).

Graf Damian K., Corona- und Crypto-Leaks – die Strafverfolgung bewegt sich nicht im rechtsfreien Raum, Gastkommentar, NZZ vom 17.2.2023, abrufbar unter <https://www.nzz.ch/meinung/was-darf-die-staatsanwaltschaft-die-corona-und-crypto-leaks-ld.1725348>, besucht am 31.3.2025 (zit. Crypto-Leaks).

Graf Damian K., Kommentierung zu Art. 32 CCC, in: Graf Damian K. (Hrsg.), Onlinekommentar, Übereinkommen über die Cyberkriminalität (Cybercrime Convention), abrufbar unter <https://onlinekommentar.ch/de/kommentare/ccc32>, besucht am 31.3.2025 (zit. OK).

Forster Marc, Marksteine der Bundesgerichtspraxis zur strafprozessualen Überwachung des digitalen Fernmeldeverkehrs, in: Festgabe Schweizerischer Juristentag 2015, Zürich 2015, S. 615 ff.

Hansjakob Thomas, Die Erhebung von Daten des Internetverkehrs – Bemerkungen zu BGer 6B_656/2015 vom 16.12.2016, *forumpoenale* 4 (2017), 252 ff. (zit. Erhebung).

Hansjakob Thomas, Überwachungsrecht der Schweiz, Kommentar zu Art. 269 ff. StPO und zum BÜPF, Zürich/Basel/Genf 2017 (zit. Überwachungsrecht).

Niggli Marcel Alexander/Heer Marianne/Wiprächtiger Hans (Hrsg.), Basler Kommentar zur Strafprozessordnung/Jugendstrafprozessordnung, 3. Aufl., Basel 2023 (zit. BSK-Bearbeiter/in, Art. ... StPO N. ...).

Roth Simon, Die grenzüberschreitende Edition von IP-Adressen und Bestandesdaten im Strafprozess, Direkter Zugriff oder Rechtshilfe?, *Jusletter* vom 17.8.2015.

Schweingruber Sandra, Cybercrime-Strafverfolgung im Konflikt mit dem Territorialitätsprinzip, *Jusletter* vom 10. November 2014.

Seger Alexander, «Grenzüberschreitender» Zugriff auf Daten im Rahmen der Budapest Konvention über Computerkriminalität, Praxisbericht zum Stand der Arbeiten des Europarats, *Zeitschrift für öffentliches Recht* 73 (2018), S. 71 ff.

Walder Stephan, Grenzüberschreitende Datenerhebung: Ist und Soll, *Kriminalistik* 8-9/2019, S. 540 ff.

I MATERIALI

Botschaft über die Genehmigung und die Umsetzung des Übereinkommens des Europarates über die Cyberkriminalität vom 18.6.2010, BBl 2010 4697 ff., abrufbar unter <https://www.fedlex.admin.ch/eli/fga/2010/813/de>, besucht am 31.3.2025.

Botschaft zum Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) vom 27.2.2013, BBl 2013 2683 ff., abrufbar unter <https://www.fedlex.admin.ch/eli/fga/2013/512/de>, besucht am 31.3.2025.

Europarat, Cybercrime Convention Committee (T-CY), The Budapest Convention on Cybercrime: benefits and impact in practice, Strassburg, 13.7.2020, abrufbar unter <https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac>, besucht am 31.3.2025 (zit. T-CY, Benefits).

Europarat, Cybercrime Convention Committee (T-CY), T-CY Guidance Note # 10, Production orders for subscriber information (Article 18 Budapest Convention), Strassburg, 28.2.2017, abrufbar unter <https://rm.coe.int/16806f943e>, besucht am 31.3.2025 (zit. T-CY Guidance Note # 10).

Europarat, Cybercrime Convention Committee (T-CY), T-CY Cloud Evidence Group, Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY, Final report, Strassburg, 16.9.2016, abrufbar unter <https://rm.coe.int/16806a495e>, besucht am 31.3.2025 (zit. T-CY, Cloud).

Europarat, Explanatory Report to the Convention on Cybercrime, Budapest, 23.11.2001, abrufbar unter <https://rm.coe.int/16800cce5b>, besucht am 31.3.2025 (zit. Explanatory Report).

ATTENZIONE: Questa versione del commentario è una traduzione automatica dell'originale. Il commentario originale è in tedesco. La traduzione è stata effettuata con www.deepl.com. Solo la versione originale fa fede. La forma tradotta del commentario non può essere citata

COMMENTO SU

Art. 25 CCC (Convenzione sulla cybercriminalità [Cybercrime Convention])

Un commentario di Miro Dangubic

CITAZIONE SUGGERITA

Miro Dangubic, Commentario all'art. 25 CCC, in: Damian K. Graf (a cura di), Commentario online alla Convenzione sulla cybercriminalità [Cybercrime Convention]

Breve citazione: OK-Dangubic, Art. 25 CCC N. XXX.

Titolo 3: Principi generali dell'assistenza giudiziaria

Art. 25 Principi generali dell'assistenza giudiziaria

¹ Le Parti si concedono reciprocamente la più ampia assistenza giudiziaria possibile al fine delle indagini o dei procedimenti per reati relativi a sistemi e dati informatici o dell'acquisizione di prove elettroniche di un reato.

² Le Parti adottano inoltre le misure legislative e di altra natura necessarie per l'adempimento degli obblighi assunti in base agli articoli 27–35.

³ In casi d'urgenza le Parti possono presentare una domanda di assistenza giudiziaria o trasmettere comunicazioni a essa relative attraverso mezzi di comunicazione veloce come il fax o la posta elettronica, a condizione che tali strumenti offrano sufficienti garanzie di sicurezza e autenticazione (se necessario ricorrendo anche alla cifratura), seguite da ulteriore conferma ufficiale se la Parte richiasta lo esige. La Parte richiasta accetta la domanda e risponde utilizzando un qualsiasi mezzo di comunicazione veloce.

⁴ Salva disposizione contraria espressamente prevista negli articoli del presente capitolo, l'assistenza giudiziaria è soggetta alle condizioni stabilite dal diritto nazionale della Parte richiasta o dai trattati di assistenza giudiziaria applicabili, inclusi i motivi in base ai quali la Parte richiasta può rifiutare la cooperazione. La Parte richiasta non può rifiutare l'assistenza giudiziaria per i reati menzionati negli articoli 2–11 adducendo come motivazione il semplice fatto che la domanda riguarda un reato da essa considerato di natura fiscale.

⁵ Se, in conformità con le disposizioni del presente capitolo, la Parte richiasta è autorizzata a subordinare l'assistenza giudiziaria alla doppia incriminazione, questa condizione sarà considerata soddisfatta se il comportamento che costituisce il reato per il quale è stata richiesta l'assistenza giudiziaria è considerato reato in base al diritto interno della Parte richiasta, a prescindere dal fatto che, nella legislazione della Parte richiasta, il reato rientri nella stessa categoria o abbia la stessa denominazione di quella prevista dal diritto della Parte richiedente.

STRUTTURA

I. Introduzione	184
II. Ambito di applicazione sostanziale della Convenzione nell'ambito dell'assistenza giudiziaria locale.....	184
A. Il reato come elemento di collegamento	185
B. Prove in formato elettronico come fattore di collegamento	185
III. Fonti giuridiche nell'assistenza giudiziaria	185
A. Disposizioni sull'assistenza giudiziaria	185
B. Diritto processuale sussidiario in Svizzera	186
IV. Obbligo di assistenza legale	186
V. Principio del massimo accomodamento	187
VI. Forme di trasmissione nell'assistenza giudiziaria	187
VII. Strutturazione del principio della doppia incriminazione	188
A. Principio della doppia incriminazione	188
B. Principio della doppia incriminazione nell'ambito di applicazione del CPC.....	188
VIII. Superare la riserva fiscale	189
IX. Mandato legislativo agli Stati contraenti	190
A. Generale	190
B. Attuazione in Svizzera.....	190
Bibliografia	190
I Materiali	191

I. INTRODUZIONE

- 1 L'art. 25 CPC riassume sotto il titolo "Principi generali dell'assistenza giudiziaria" varie disposizioni relative all'assistenza giudiziaria su scala ridotta nell'ambito di applicazione del CPC. In particolare, l'articolo contiene disposizioni riguardanti
 - l'ambito materiale di applicazione del TCC (cpv. 1),
 - le fonti giuridiche rilevanti nei procedimenti di assistenza giudiziaria (cpv. 4),
 - l'obbligo di fornire assistenza legale ai minori (cpv. 1),
 - il principio del massimo accomodamento (cpv. 1),
 - le possibili forme di trasmissione nei procedimenti di assistenza giudiziaria (par. 3),
 - l'organizzazione del principio della doppia incriminazione (cpv. 5) e la violazione della riserva fiscale (cpv. 6).
 - la violazione della riserva fiscale (cpv. 4).
- 2 Inoltre, l'art. 25 cpv. 2 CPC contiene un mandato legislativo agli Stati contraenti.
- 3 La CCC ha lo scopo di integrare i trattati e gli accordi bilaterali o multilaterali esistenti tra le parti contraenti (in particolare anche l'EUeR) e quindi di accelerare e semplificare le procedure di assistenza giudiziaria. La sua concezione come convenzione complementare ha un forte impatto sul contenuto normativo e sulla densità della regolamentazione relativa all'assistenza giudiziaria su piccola scala.

II. AMBITO DI APPLICAZIONE SOSTANZIALE DELLA CONVENZIONE NELL'AMBITO DELL'ASSISTENZA GIUDIZIARIA LOCALE

- 4 L'ambito di applicazione sostanziale del CCL in relazione all'assistenza reciproca locale è disciplinato dall'art. 25 cpv. 1 del CCL e presenta due fattori di collegamento alternativi: Da un lato, può essere collegato al reato oggetto

di indagine ("reati relativi a sistemi e dati informatici") e, dall'altro, alle prove da raccogliere ("prove in formato elettronico").

A. Il reato come elemento di collegamento

Da un lato, l'ambito di applicazione materiale si applica se vi è il sospetto che sia stato commesso un reato di cui agli artt. 2-11 CPC. Dall'altro lato, il campo di applicazione materiale si applica ai reati commessi per mezzo di un sistema informatico, indipendentemente dal reato effettivamente commesso. Il reato di "sistema informatico" è definito all'art. 1 lett. a CPC come segue: "un dispositivo o un gruppo di dispositivi interconnessi o collegati che, singolarmente o in combinazione, eseguono un'elaborazione automatica di dati sulla base di un programma".

Nell'esame prima facie di questo campo di applicazione materiale da parte delle autorità di assistenza giudiziaria, si deve tenere conto in particolare di quanto segue: Alcuni elementi dell'ambito di applicazione materiale sono in linea di principio parte dei fatti giuridicamente rilevanti da chiarire nel contesto dell'indagine penale estera; in alcune circostanze, sono proprio questi punti che le misure probatorie richieste sono destinate a chiarire. Di conseguenza, non si devono porre requisiti elevati alla descrizione di questi elementi dei fatti.

B. Prove in formato elettronico come fattore di collegamento

Se nell'ambito dell'assistenza giudiziaria in materia penale devono essere raccolte prove che si presume siano in formato elettronico, il campo di applicazione materiale del CCC si applica indipendentemente dal reato oggetto di indagine. Le prove in formato elettronico possono essere, in particolare, dati.

III. FONTI GIURIDICHE NELL'ASSISTENZA GIUDIZIARIA

A. Disposizioni sull'assistenza giudiziaria

I procedimenti di assistenza giudiziaria nell'ambito del Codice penale sono disciplinati principalmente dai trattati internazionali in materia e dal Codice penale. Se questi trattati internazionali non disciplinano espressamente o implicitamente determinate questioni, si applicano le disposizioni nazionali

(art. 25 cpv. 4 CPC). In Svizzera, l'AIMP e l'OAIMP sono autorevoli per l'assistenza giudiziaria in materia penale (art. 1 cpv. 1 AIMP). Il principio del favor rei - anch'esso sancito dall'art. 25 cpv. 1 CPC - stabilisce che le disposizioni nazionali si applicano anche se impongono requisiti meno severi all'assistenza giudiziaria. Di conseguenza, le disposizioni del Codice di procedura penale si applicano nei procedimenti di assistenza giudiziaria solo se rappresentano la norma più favorevole dal punto di vista dello Stato richiedente.

B. Diritto processuale sussidiario in Svizzera

- 9 Se le disposizioni sull'assistenza giudiziaria mancano di disposizioni procedurali pertinenti, il CPP e la PA si applicano mutatis mutandis nei procedimenti di assistenza giudiziaria in Svizzera. Il Codice di procedura penale svizzero fa fede nei procedimenti di assistenza giudiziaria se l'AIMP vi fa riferimento direttamente o in relazione ad atti processuali penali ai sensi dell'art. 63 e segg. AIMP. Negli altri casi, la PA funge da diritto processuale sussidiario.

IV. OBBLIGO DI ASSISTENZA LEGALE

- 10 Ai sensi dell'art. 25 cpv. 1 CPC, lo Stato richiesto è obbligato, se sono soddisfatte tutte le condizioni per l'assistenza giudiziaria, a prestare l'assistenza giudiziaria minore se gli viene richiesta da una parte contraente. Tuttavia, tale obbligo non implica che lo Stato richiedente abbia lo status di parte o i rimedi legali nel contesto del procedimento di assistenza giudiziaria. Eventuali posizioni divergenti degli Stati in merito alla questione se le condizioni per l'assistenza giudiziaria in materia penale siano soddisfatte e se l'assistenza giudiziaria debba essere fornita devono essere risolte a livello diplomatico.
- 11 Nel caso dell'assistenza giudiziaria extracontrattuale in materia penale, non sussiste il diritto alla cooperazione intergovernativa in materia penale (cfr. art. 1 cpv. 4 AIMP).

V. PRINCIPIO DEL MASSIMO ACCOMODAMENTO

L'art. 25 cpv. 1 CCC obbliga lo Stato richiesto a soddisfare le richieste di assistenza reciproca nell'ambito di applicazione del CCC "nella misura più ampia possibile" (il cosiddetto principio della massima collaborazione). 12

Il principio del massimo accomodamento è un principio generalmente riconosciuto di assistenza giudiziaria in materia penale che non ha carattere meramente programmatico. Il principio include il già citato principio del favor rei. In pratica, il principio del favor rei si applica in tutti i procedimenti di assistenza giudiziaria, anche se non vi è alcun obbligo in tal senso ai sensi dei trattati internazionali. Esso stabilisce che il diritto nazionale non può rendere l'assistenza giudiziaria in materia penale più difficile di quanto non lo sia il diritto dei trattati internazionali, ma può renderla più facile. 13

Il principio del massimo accomodamento riguarda anche la portata dell'assistenza legale da fornire. Esso consente di interpretare generosamente le misure richieste in una domanda di assistenza giudiziaria e di consegnare all'autorità richiedente tutte le prove potenzialmente rilevanti per il procedimento penale straniero, anche se l'autorità richiedente non lo ha esplicitamente richiesto. 14

VI. FORME DI TRASMISSIONE NELL'ASSISTENZA GIUDIZIARIA

Secondo l'AIMP, le richieste di assistenza giudiziaria rivolte alla Svizzera devono essere generalmente inviate per iscritto all'Ufficio federale di giustizia. Tuttavia, diversi trattati europei consentono anche la comunicazione diretta tra gli organi giudiziari competenti (di solito le procure) e alternative alla corrispondenza scritta. 15

Nell'ambito di applicazione del Codice penale, l'art. 25 cpv. 3 del Codice penale autorizza l'uso di "mezzi di comunicazione rapidi, compresi il fax e la posta elettronica" in casi urgenti. Ciò si applica non solo alle richieste di assistenza giudiziaria, ma a tutta l'assistenza giudiziaria. Lo scopo di questa disposizione è quello di accelerare i procedimenti di assistenza giudiziaria e, in particolare, di consentire una rapida acquisizione delle prove per contrastare il rischio di perdita delle stesse. La richiesta di assistenza 16

giudiziaria deve essere presentata per iscritto su esplicita richiesta dello Stato richiesto.

- 17 L'urgenza temporale è data se esiste il rischio di perdita di prove con la trasmissione in forma scritta. Ciò vale in particolare se i dati devono essere raccolti ai fini dell'assistenza giudiziaria.
- 18 Non esiste un *numerus clausus* per quanto riguarda i mezzi di comunicazione che possono essere utilizzati. In pratica, vengono utilizzati in particolare la posta elettronica, il fax e le piattaforme di file-sharing statali. Tuttavia, le richieste di assistenza legale possono essere presentate anche per telefono.
- 19 I relativi standard di sicurezza e di autenticazione derivano dagli ordinamenti giuridici nazionali o dalle linee guida e dalla prassi delle autorità competenti.

VII. STRUTTURAZIONE DEL PRINCIPIO DELLA DOPPIA INCRIMINAZIONE

- 20 L'art. 25 cpv. 5 CPC disciplina l'organizzazione del principio della doppia incriminazione.

A. Principio della doppia incriminazione

- 21 La doppia incriminazione è un principio classico della cooperazione internazionale. Esso stabilisce che l'assistenza giudiziaria in materia penale è concessa solo per i reati punibili secondo la legge dello Stato richiedente e di quello richiesto. Il principio della doppia incriminazione fa parte dell'ordine pubblico svizzero ed è stato garantito di conseguenza in tutti i trattati bilaterali e (tramite riserve) nelle convenzioni multilaterali di assistenza giudiziaria, anche per quanto riguarda il campo di applicazione del CCC.

B. Principio della doppia incriminazione nell'ambito di applicazione del CPC

- 22 Se le misure che richiedono coercizione procedurale devono essere applicate nel contesto di un procedimento di assistenza giudiziaria, il principio della doppia incriminazione si applica all'ambito di applicazione del CCC. Tuttavia, esistono anche delle eccezioni a questo principio.

In base ai principi generali, la responsabilità penale ai sensi della legge dello Stato richiedente - anch'essa rientrante nell'ambito di applicazione della Convenzione - non deve essere esaminata in linea di principio nei procedimenti di assistenza giudiziaria, fatti salvi i casi di evidente abuso. 23

Per quanto riguarda la questione della doppia incriminazione ai sensi del diritto svizzero, l'autorità di esecuzione esamina se l'insieme dei fatti descritti nella richiesta di assistenza giudiziaria possa essere prima facie ricondotto a una disposizione penale svizzera. L'art. 25 cpv. 5 CCC stabilisce, da un lato, che è sufficiente che i fatti descritti nella richiesta di assistenza giudiziaria siano riconducibili a un'unica fattispecie di reato ai sensi del diritto svizzero - non è necessario esaminare ulteriormente se possano essere soddisfatte anche altre fattispecie di reato. D'altra parte, stabilisce che la doppia incriminazione non richiede norme penali identiche nello Stato richiedente e in quello richiesto. Di conseguenza, il contenuto del cpv. 5 corrisponde già alla pratica corrente in Svizzera. 24

VIII. SUPERARE LA RISERVA FISCALE

Tradizionalmente, numerose fonti del diritto - sia nazionali che internazionali - contengono una cosiddetta riserva fiscale. Ad esempio, l'art. 3 cpv. 3 dell'AIMP stabilisce che l'assistenza legale accessoria nei procedimenti per evasione fiscale è esclusa in linea di principio. 25

La seconda frase dell'art. 25 cpv. 4 CPC ha lo scopo di garantire che eventuali riserve fiscali non ostacolino l'assistenza giudiziaria nell'ambito di applicazione del CPC se sono in corso indagini per reati ai sensi degli artt. 2-11 CPC. Poiché i reati descritti nell'art. 2-11 del Codice penale non sono reati fiscali, è probabile che la rilevanza pratica di questa disposizione sia piuttosto limitata. Nel migliore dei casi, si potrebbero considerare delle costellazioni di concorso ideale: l'autore del reato commette sia un reato fiscale non ammissibile all'assistenza legale sia un reato penale ai sensi dell'art. 2-11 CCC con un unico atto o con un atto uniforme e collegato. In questo caso, la riserva fiscale sarebbe sempre violata. 26

IX. MANDATO LEGISLATIVO AGLI STATI CONTRAENTI

A. Generale

- 27 L'art. 25 cpv. 2 del CDC obbliga gli Stati contraenti a garantire, nell'organizzazione dei loro sistemi giuridici nazionali, l'esistenza di strumenti nazionali per l'attuazione delle disposizioni degli artt. 27-35 del CDC. Questa norma rappresenta quindi in primo luogo un cosiddetto mandato legislativo di diritto internazionale.
- 28 L'obbligo è fondamentalmente rivolto al legislatore e richiede allo Stato parte di agire attivamente - se il diritto interno non soddisfa (ancora) i requisiti. Gli Stati parte che dispongono già degli strumenti giuridici necessari non sono tenuti ad adottare misure legislative.

B. Attuazione in Svizzera

- 29 Come intendiamo qui, le disposizioni degli artt. 27-35 CDC sono generalmente da considerarsi autoesecutive. Per quanto riguarda la loro applicabilità ed esecutività a livello nazionale, il legislatore ha ravvisato la necessità di intervenire solo per quanto riguarda gli artt. 30 e 33 del TUB.
- 30 Per attuare l'art. 30 CCC (divulgazione immediata di dati sul traffico protetti) e l'art. 33 CCC (assistenza legale nella raccolta di dati sul traffico in tempo reale), l'art. 18b AIMP è stato inserito nella legge con la nota marginale "Dati elettronici" dal decreto federale del 18 marzo 2011.

BIBLIOGRAFIA

Böhi Simon, Kommentierung zu Art. 18b IRSG, in: Niggli Marcel Alexander/Heimgartner Stefan (Hrsg.), Basler Kommentar, Internationales Strafrecht, IRSG, GwÜ, Basel 2015.

Dangubic Miro, Parteistellung und Parteirechte bei der rechtshilfeweisen Herausgabe von Kontoinformationen, *forumpoenale* 2018, S. 112–117.

Dangubic Miro/Clerc Yves, Art. 80dbis – ein Überblick, *forumpoenale* 2022, S. 287–292.

Donatsch Andreas/Heimgartner Stefan/Meyer Frank/Simonek Madeleine, *Internationale Rechtshilfe*, 2. Aufl., Zürich et al. 2015.

Donatsch Andreas/Godenzi Gunhild/Tag Brigitte, Strafrecht I, Verbrechenslehre, 10. Aufl., Zürich 2022.

Garré Roy, Kommentierung zu Art. 35 IRSG, in: Niggli Marcel Alexander/Heimgartner Stefan (Hrsg.), Basler Kommentar, Internationales Strafrecht, IRSG, GwÜ, Basel 2015.

Graf Damian K., in: Ackermann Jürg-Beat (Hrsg.), Wirtschaftsstrafrecht der Schweiz, Hand- und Studienbuch, 2. Aufl., Bern 2021.

Graf Damian K., Kommentierung zu Art. 32 CCC, in: Graf Damian K. (Hrsg.), Onlinekommentar, Übereinkommen über die Cyberkriminalität (Cybercrime Convention), abrufbar unter <https://onlinekommentar.ch/de/kommentare/ccc32>, besucht am 21.11.2023.

Heimgartner Stefan, Kommentierung zu Art. 64 IRSG, in: Niggli Marcel Alexander/Heimgartner Stefan (Hrsg.), Basler Kommentar, Internationales Strafrecht, IRSG, GwÜ, Basel 2015.

Heimgartner Stefan/Niggli Marcel Alexander, Kommentierung zu Einführung IRSG, in: Niggli Marcel Alexander/Heimgartner Stefan (Hrsg.), Basler Kommentar, Internationales Strafrecht, IRSG, GwÜ, Basel 2015.

Kocher Martin, Kommentierung zu Art. 3 IRSG, in: Niggli Marcel Alexander/Heimgartner Stefan (Hrsg.), Basler Kommentar, Internationales Strafrecht, IRSG, GwÜ, Basel 2015.

Popp Peter, Grundzüge der internationalen Rechtshilfe in Strafsachen, Basel et al. 2001.

I MATERIALI

Botschaft über die Genehmigung und die Umsetzung des Übereinkommens des Europarates über die Cyberkriminalität vom 18.6.2010, BBl 2010 4697 ff., abrufbar unter <https://www.admin.ch/opc/de/federal-gazette/2010/4697.pdf>, besucht am 21.10.2023 (zit. Botschaft 2010).

Explanatory Report to the Convention on Cybercrime, European Treaty Series – No. 185, Budapest, 23.XI.2001, abrufbar unter <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cce5b>, besucht am 21.10.2023 (zit. Explanatory Report).

ATTENZIONE: Questa versione del commentario è una traduzione automatica dell'originale. Il commentario originale è in tedesco. La traduzione è stata effettuata con www.deepl.com. Solo la versione originale fa fede. La forma tradotta del commentario non può essere citata

COMMENTO SU

Art. 27 CCC (Convenzione sulla cybercriminalità [Cybercrime Convention])

Un commentario di Jan Reinhardt

CITAZIONE SUGGERITA

Jan Reinhardt, Commentario all'art. 27 CCC, in: Damian K. Graf (a cura di), Commentario online alla Convenzione sulla cybercriminalità [Cybercrime Convention]

Breve citazione: OK-Reinhardt, art. 27 CCC N. XXX.

Titolo 4:

Procedure relative alle domande di assistenza giudiziaria in assenza di accordi internazionali applicabili

Art. 27 Procedure di assistenza giudiziaria in assenza di accordi internazionali applicabili

¹ Qualora tra la Parte richiedente e la Parte richiesta non siano in vigore trattati di assistenza giudiziaria o accordi fondati su normative uniformi o reciproche, si applicano le disposizioni dei paragrafi 2–9. Tali

disposizioni non si applicano qualora vi sia un trattato, un accordo o una normativa simile in vigore, a meno che le Parti interessate decidano di applicare al loro posto i paragrafi 2–9 in tutto o in parte.

² a. Le Parti designano una o più autorità centrali incaricate di inviare le domande di assistenza giudiziaria e di rispondervi, nonché di eseguire o trasmettere tali domande alle autorità competenti per l'esecuzione;

b. le autorità centrali comunicano direttamente tra loro;

c. al momento della firma o del deposito dello strumento di ratifica, di accettazione, di approvazione o di adesione, le Parti comunicano al Segretario generale del Consiglio d'Europa il nome e l'indirizzo delle autorità designate in applicazione del presente paragrafo;

d. il Segretario generale del Consiglio d'Europa istituisce e tiene aggiornato un registro delle autorità designate dalle Parti. Le Parti assicurano la costante correttezza dei dati riportati nel registro.

³ Le domande di assistenza giudiziaria presentate in base al presente articolo sono eseguite in conformità con le procedure specificate dalla Parte richiedente,

⁴ In aggiunta ai motivi di rifiuto previsti dall'articolo 25 paragrafo 4, la Parte richiesta può rifiutare l'assistenza se:

a. la domanda riguarda un reato che la Parte richiesta considera di natura politica o connesso a un reato politico; o

b. la Parte richiesta ritiene che l'esecuzione della domanda possa pregiudicare la sua sovranità, la sua sicurezza, il suo ordine pubblico o altri suoi interessi essenziali.

⁵ La Parte richiesta può sospendere l'esecuzione di una domanda se teme che essa possa pregiudicare indagini o procedimenti condotti dalle proprie autorità.

⁶ Prima di rifiutare o sospendere l'assistenza giudiziaria, la Parte richiesta valuta, se del caso dopo aver consultato la Parte richiedente, se la domanda possa essere parzialmente eseguita o subordinata alle condizioni che ritenga necessarie.

⁷ La Parte richiesta informa prontamente la Parte richiedente del seguito che intende dare alla domanda di assistenza giudiziaria. Motiva l'eventuale rifiuto o sospensione della domanda. Inoltre informa la Parte richiedente delle motivazioni che rendono impossibile o possono ritardare in modo significativo l'esecuzione dell'assistenza giudiziaria.

⁸ La Parte richiedente può esigere che la Parte richiesta mantenga confidenziali le domande presentate in base al presente capitolo e il relativo contenuto, salvo che l'esecuzione della domanda non imponga altrimenti. Qualora la Parte richiesta non possa soddisfare il requisito di confidenzialità, ne informa prontamente l'altra Parte, che decide se la domanda vada comunque eseguita.

⁹ a. In caso di urgenza, le autorità giudiziarie della Parte richiedente possono indirizzare le domande di assistenza giudiziaria o le relative comunicazioni direttamente alle omologhe autorità della Parte richiesta. In tale caso, l'autorità centrale della Parte richiedente trasmette contemporaneamente una copia della domanda o delle comunicazioni all'autorità centrale della Parte richiesta.

b. Le domande o comunicazioni di cui al presente paragrafo possono essere effettuate per il tramite dell'Organizzazione internazionale di polizia giudiziaria (Interpol).

c. Qualora venga presentata una domanda in base alla lettera a e l'autorità ricevente non sia competente a trattarla, essa la inoltra all'autorità nazionale competente e ne informa direttamente la Parte richiedente.

d. Le domande o le comunicazioni effettuate in base al presente paragrafo che non implicano misure coercitive possono essere trasmesse direttamente dalle autorità competenti della Parte richiedente alle autorità competenti della Parte richiesta.

e. Al momento della firma o del deposito dello strumento di ratifica, di accettazione, di approvazione o di adesione, le Parti possono comunicare al Segretario generale del Consiglio d'Europa che, per ragioni di efficienza, le domande effettuate in base al presente

STRUTTURA

I. Considerazioni generali.....	197
II. Rapporto con altre disposizioni	197
III. Disposizioni relative all'assistenza giudiziaria	199
A. Istituzione di autorità (cpv. 2)	199
B. Prescrizioni relative alle modalità di esecuzione (cpv. 3).....	200
C. Obiezioni contro l'esecuzione	202
1. Motivi supplementari di rifiuto (cpv. 4).....	202
2. Rinvio dell'assistenza giudiziaria (cpv. 5).....	203
3. Condizione come presupposto per il rifiuto e il rinvio (cpv. 6).....	204
D. Obblighi di comunicazione (cpv. 7).....	204
E. Riservatezza (cpv. 8).....	205
F. «Procedura accelerata» (cpv. 9)	207
IV. Tutela giuridica	208
Bibliografia	209
I materiali.....	210

I. CONSIDERAZIONI GENERALI

L'art. 27 CCC completa il principio generale dell'assistenza giudiziaria di cui ¹ all'art. 25 cpv. 1 CCC e garantisce un **quadro istituzionale minimo** per l'assistenza giudiziaria di modesta entità. La norma impedisce che tra due parti contraenti si debba ricorrere all'assistenza giudiziaria non convenuta e serve così al principio dell'efficacia di cui all'art. 25 cpv. 1 CCC.

Oltre all'obbligo di designare determinate autorità, la norma contiene un ² obbligo più dettagliato **di eseguire le richieste di assistenza giudiziaria**. In tal senso, essa è autoesecutiva secondo la concezione monistica svizzera. Per le singole misure oggetto della richiesta deve tuttavia esistere, come nell'assistenza giudiziaria non convenzionale ai sensi dell'AIMP, una base di autorizzazione nel diritto procedurale nazionale. Dall'art. 25 cpv. 2 CCC discende inoltre che gli Stati contraenti devono adeguare il proprio ordinamento giuridico in modo che non ostacoli la procedura prevista dagli articoli della sezione. A tale proposito, non è stata ravvisata alcuna necessità in relazione all'art. 27 CCC.

II. RAPPORTO CON ALTRE DISPOSIZIONI

L'art. 27 CCC stabilisce unicamente una procedura per le richieste di ³ assistenza giudiziaria. Il presupposto è l'apertura del campo di applicazione definito all'art. 25 cpv. 1. Questo comprende tutte le procedure relative a sistemi e dati informatici nonché l'assunzione di prove in forma elettronica anche per altri reati. Proprio quest'ultimo aspetto crea un **ampio campo di applicazione**. Il secondo protocollo aggiuntivo alla CCC contiene diversi rinvii parziali all'art. 27 CCC, segnatamente all'art. 3 cpv. 2 lett. a, all'art. 7 cpv. 5 lett. a, all'art. 8 cpv. 8, all'art. 10 cpv. 7 e all'art. 11 cpv. 2 lett. b. Tuttavia, la Svizzera non ha ancora né firmato né ratificato questo protocollo aggiuntivo.

L'art. 25 CCC disciplina, oltre al campo di applicazione, i principi ⁴ dell'assistenza giudiziaria secondo la CCC. Nei suoi cpv. 2 e 4 rimanda in via prioritaria alle disposizioni della CCC e, in via sussidiaria, al diritto nazionale, in Svizzera in particolare all'AIMP, e in via subordinata alla PA e al CPP. L'art. 27 CCC è quindi, dal punto di vista della CCC, **prevalente rispetto alle norme del diritto nazionale**. Spetta al diritto nazionale stabilire in che misura tale prevalenza sussista anche dal suo punto di vista. Per la Svizzera si

può presumere una prevalenza di principio dell'art. 27 CCC. Considerate le disposizioni fondamentali e prevalentemente organizzative dell'art. 27 CCC, è comunque improbabile che tale disposizione entri in conflitto con il diritto nazionale. Essa crea piuttosto uno standard minimo che non osta a una regolamentazione dettagliata e più ampia da parte del diritto nazionale.

- 5 L'articolo 27 cpv. 1, commi 1 e 2 CCC stabilisce, in conformità con il titolo del quarto titolo – «Procedura per le richieste di assistenza giudiziaria **in assenza di accordi internazionali applicabili**» –, che le disposizioni dell'articolo sono applicabili a ogni singola richiesta di assistenza giudiziaria solo se tra lo Stato richiedente e lo Stato richiesto non è in vigore un trattato (bilaterale) di assistenza giudiziaria o un accordo (multilaterale) o se le parti, nonostante l'esistenza di un trattato di assistenza giudiziaria, concordano di applicare in tutto o in parte l'art. 27 CCC. Al di là del testo letterale, un altro accordo limitato a un settore specifico non dovrebbe essere sufficiente. Si intende piuttosto un accordo generale di assistenza giudiziaria che garantisca l'assistenza giudiziaria (minore) anche nell'ambito di applicazione dell'art. 25 cpv. 1 CCC. Se esiste un contratto di questo tipo, l'art. 27 CCC non è applicabile, nemmeno in parte, ad esempio per quanto riguarda i motivi di rifiuto supplementari di cui all'art. 27 cpv. 4 CCC, salvo accordo tra le parti contraenti. Ciò chiarisce che l'art. 27 CCC stabilisce solo uno standard minimo che non osta a un **ulteriore vincolo degli Stati contraenti in altri accordi**. Non si tratta di una disposizione essenziale della CCC come l'art. 25 cpv. 4, seconda frase, CCC o l'art. 29 CCC, che secondo la sistematica della convenzione non sono derogabili.
- 6 Il campo di applicazione effettivo dell'art. 27 CCC è limitato per la Svizzera, come per molti altri Stati contraenti. Esso è innanzitutto notevolmente limitato dalla Convenzione europea del 20 aprile 1959 relativa all'assistenza giudiziaria in materia penale. Questa convenzione offre una regolamentazione completa e prevalente tra gli Stati membri firmatari del Consiglio d'Europa. A ciò si aggiungono i trattati bilaterali di assistenza giudiziaria della Svizzera, ad esempio con gli Stati Uniti d'America, il Canada o il Perù. Questi trattati disciplinano in modo esaustivo l'assistenza giudiziaria reciproca in materia penale e non prevedono l'applicazione complementare dell'art. 27 CCC, che non trova quindi applicazione. La normativa è applicabile alla Svizzera **principalmente nei rapporti con molti Stati africani e latinoamericani, nonché tra la Svizzera e il Giappone**. Gli Stati senza accordi applicabili o

trattati bilaterali sono attualmente (stato al 12.4.2025): Argentina, Benin, Brasile, Capo Verde, Costa Rica, Costa d'Avorio, Repubblica Dominicana, Isole Figi, Ghana, Grenada, Giappone, Camerun, Kiribati, Colombia, Marocco, Mauritius, Nigeria, Panama, Senegal, Sierra Leone, Sri Lanka, Tonga e Tunisia. Infine, la procedura prevista dalla CCC dovrebbe trovare applicazione anche nei rapporti con il Paraguay. A tal proposito esiste solo un trattato di estradizione, ma non un trattato completo in materia di assistenza giudiziaria limitata. Per quanto riguarda l'assunzione e la conservazione delle prove, solo gli articoli 16 e 17 del trattato contengono disposizioni relative all'audizione dei testimoni. Inoltre, l'ambito di applicazione del trattato di estradizione è limitato, all'articolo 2, a cui si fa riferimento negli articoli successivi, a determinati reati elencati. L'elenco comprende, ad esempio sotto forma di frode ai sensi dell'articolo 2 n. 18 del trattato, solo una minima parte dei reati punibili ai sensi degli articoli 2 e seguenti della CCC, il che non sorprende vista la data di conclusione del trattato nel 1906. Anche nei rapporti tra la Svizzera e il Ruanda dovrebbe trovare applicazione l'articolo 27 della CCC. Gli articoli 13 e 14 del trattato di estradizione tra la Svizzera e il Belgio, che restano applicabili in materia, contengono solo disposizioni rudimentali sull'assistenza giudiziaria limitata attraverso i canali diplomatici. Lo scopo dell'articolo 27 CCC, che è quello di garantire uno standard minimo efficace nel suo ambito di applicazione, richiede anche in questo caso l'applicazione delle disposizioni più ampie di tale articolo.

I conflitti normativi all'interno della CCC dovrebbero essere risolti secondo i 7 principi generali di interpretazione, in particolare secondo il principio della *lex specialis*.

III. DISPOSIZIONI RELATIVE ALL'ASSISTENZA GIUDIZIARIA

A. Istituzione di autorità (cpv. 2)

La comunicazione tramite autorità centrali, consueta nel settore 8 dell'assistenza giudiziaria, ha lo scopo di fornire alla parte richiedente un **interlocutore centrale** e di accelerare così l'azione penale internazionale, aspetto particolarmente importante nel caso della criminalità informatica. Allo stesso tempo, deve essere garantita la parità di trattamento delle richieste in entrata e in uscita. La comunicazione tramite autorità centrali evita la

comunicazione inefficiente tramite canali diplomatici, che sarebbe altrimenti necessaria in caso di assistenza giudiziaria non convenzionata.

- 9 Il Consiglio federale ha designato l'**Ufficio federale di giustizia** come autorità competente. Per le richieste di assistenza giudiziaria basate sulla CCC non vi è quindi alcuna deroga all'art. 27 cpv. 2 AIMP. L'elenco aggiornato delle autorità competenti di tutti gli Stati contraenti è disponibile in inglese sul sito Internet del Consiglio d'Europa.

B. Prescrizioni relative alle modalità di esecuzione (cpv. 3)

- 10 Il cpv. 3 corrisponde in larga misura all'art. 65 AIMP e alle disposizioni contenute nei trattati bilaterali di assistenza giudiziaria. La disposizione mira a garantire che le prove ottenute mediante assistenza giudiziaria possano essere utilizzate nel procedimento penale dello Stato richiedente. Il diritto processuale penale dei singoli Stati contraenti presenta in parte notevoli differenze per quanto riguarda i requisiti per l'assunzione delle prove. A titolo di esempio si cita il requisito generale della certificazione delle testimonianze, cfr. anche art. 65 cpv. 1 lett. a AIMP. Se lo Stato richiesto, che non conosce tale requisito, tenesse conto esclusivamente del proprio diritto processuale, sussisterebbe il rischio dell'**inutilizzabilità nello Stato richiedente** e l'assistenza giudiziaria mancherebbe il suo scopo. Lo Stato richiesto applica infatti regolarmente il proprio diritto processuale penale, cfr. art. 12 e art. 63 cpv. 1 AIMP.
- 11 Il principio dell'efficacia dell'assistenza giudiziaria non è tuttavia garantito in modo assoluto. L'esecuzione secondo la procedura indicata dallo Stato richiedente è infatti subordinata alla **compatibilità con il diritto dello Stato** richiesto, cfr. anche art. 65 cpv. 2 AIMP. Quest'ultimo può quindi – fatta salva l'eventuale possibilità di rifiutare l'assistenza giudiziaria nel suo complesso – applicare il proprio diritto procedurale nella misura in cui la procedura prescritta dallo Stato richiedente è incompatibile con il suo diritto nazionale. Tenuto conto del testo inglese («except where») e francese («sauf lorsqu'elle») e dello scopo indicato della deroga, quest'ultima dovrebbe sempre riferirsi solo a singole disposizioni. Lo Stato richiesto non può quindi applicare la propria procedura nazionale nel suo complesso perché una singola disposizione è incompatibile con il suo diritto. In base al testo citato, al principio dell'art. 25 cpv. 1 CCC e allo spirito dell'art. 27 cpv. 6 CCC, sarebbe addirittura opportuno ridurre, per quanto possibile, la disposizione

incompatibile alla misura ancora compatibile e massimizzare così la probabilità di utilizzabilità nello Stato richiedente. Una soluzione pratica consiste nel consultare le autorità competenti ai sensi del cpv. 2.

È molto importante distinguere tra un modo di esecuzione **incompatibile con** il diritto nazionale e un modo di esecuzione **semplicemente non previsto** da quest'ultimo, poiché il rifiuto non può essere basato solo su quest'ultimo fatto. In ogni caso, le disposizioni di rango costituzionale, come quelle relative alla laicità in relazione ai requisiti di giuramento religioso, giustificano il rifiuto. Viceversa, la semplice diversità della normativa di diritto interno non è naturalmente sufficiente. Da ciò devono essere distinte, mediante interpretazione nel singolo caso, le norme di diritto semplice che ostano espressamente all'atto concreto di esecuzione. Il fattore decisivo dovrebbe risiedere nella questione se la formalità richiesta costituisca un'ulteriore ingerenza sostanziale nei diritti individuali per la quale manca una base legale. 12

L'intenzione degli Stati contraenti dovrebbe corrispondere a un'applicazione più restrittiva del cpv. 3 rispetto all'art. 65 cpv. 2 AIMP. Ciò si evince anche dal fatto che il CCC non contiene l'ulteriore criterio estensivo dello svantaggio sostanziale. Inoltre, l'art. 25 CCC stabilisce anche un regime di assistenza giudiziaria più rigoroso per il settore particolarmente internazionalizzato della criminalità informatica. 13

Allo stesso tempo, il confronto con il cpv. 4 lett. a mostra che non è voluta una riduzione a una riserva di puro *ordine pubblico* per il potere di rifiuto limitato di cui al cpv. 3. La riserva va quindi inquadrata tra la disposizione ampia dell'art. 65 cpv. 2 AIMP e un principio di *ordine pubblico* puro, come quello contenuto ad esempio nel § 73 cpv. 1 dell'IRG tedesco. Di conseguenza, una richiesta può e deve essere respinta se per il suo adempimento sarebbero necessari **interventi sostanziali nei diritti individuali** senza base legale e contrari alla ponderazione dei beni effettuata dal legislatore. 14

Nella misura in cui il diritto procedurale nazionale prevede **ulteriori requisiti** per la misura da eseguire, questi devono essere rispettati dalle autorità esecutive dello Stato richiesto, cfr. anche art. 12 cpv. 1 AIMP. 15

C. Obiezioni contro l'esecuzione

1. Motivi supplementari di rifiuto (cpv. 4)

- 16 Nella procedura ai sensi dell'art. 27 CCC si applica innanzitutto l'art. 25 cpv. 4 CCC. Anche in questo caso si applica quindi il rinvio ai motivi di rifiuto previsti dal diritto nazionale o da un trattato di assistenza giudiziaria applicabile, fermo restando che il rifiuto è inammissibile *solo e unicamente* in base alla qualificazione come reato fiscale. L'art. 27 cpv. 4 CCC fa riferimento all'art. 25 cpv. 4 CCC e stabilisce due motivi di rifiuto supplementari: il perseguimento di **reati politici** e il *principio dell'ordine pubblico*. Lo Stato richiesto può quindi invocare tali motivi di rifiuto anche se il diritto nazionale non li prevede. In caso di applicazione di una convenzione internazionale, l'art. 27 CCC non trova invece applicazione, conformemente al suo cpv. 1.
- 17 Alla luce della sistematica della CCC, secondo la quale nel caso dell'art. 27 CCC intervengono regolarmente i motivi di rifiuto previsti dal diritto nazionale, non è del tutto chiaro a prima vista quale sia il valore aggiunto pratico offerto dai motivi di rifiuto supplementari. Uno Stato che non prevede tali limiti nel proprio diritto nazionale non li invocherà regolarmente nemmeno nel procedimento ai sensi della CCC, poiché il rigetto ai sensi del cpv. 4 è a discrezione dello Stato richiesto. Il significato dovrebbe derivare dal fatto che, in applicazione del principio della massima assistenza giudiziaria, gli Stati hanno convenuto di fare ricorso ai motivi di rifiuto previsti dal diritto nazionale non menzionati nel cpv. 4 solo in casi eccezionali nell'ambito di applicazione della CCC. Il cpv. 4 ha quindi un effetto **chiarchificatorio e simbolico**. La disposizione mostra che i motivi di rifiuto citati rimangono comunque validi in quanto espressione della visione del mondo nazionale. L'accordo sulla non applicazione di altri motivi di rifiuto nei casi normali dovrebbe tuttavia essere vincolante in primo luogo sul piano politico, anche perché non è stato inserito nel testo della Convenzione.
- 18 Per la Svizzera, oltre all'AIMP, dovrebbe sussistere al massimo un **ambito di applicazione** limitato per i motivi di rikusazione supplementari in applicazione diretta del cpv. 4. Per i reati politici si applica il motivo di rikusazione di cui all'art. 3 cpv. 1 AIMP. Si deve presumere che anche l'art. 27 cpv. 4 lett. a CCC comprenda sia i reati politici assoluti che quelli relativi. Considerata la regolamentazione cauta e ampiamente rinviata al diritto nazionale contenuta nella CCC, nonché la qualificazione soggettiva e

divergente tra gli Stati di un reato come politico o non politico, non dovrebbe essere data un'interpretazione autonoma. Spetta piuttosto allo Stato richiesto definire il motivo di rifiuto, salvo in caso di abuso di diritto. In caso di esclusione ai sensi dell'art. 3 cpv. 2 AIMP, non è prevedibile nemmeno il rifiuto ai sensi dell'art. 27 cpv. 4 lett. a CCC.

La riserva di *ordre public* trova parziale espressione nell'art. 2 AIMP. In 19 quanto principio generale del diritto internazionale e in considerazione dell'interpretazione conforme alla Costituzione dell'AIMP, in particolare della clausola generale dell'art. 2 lett. d AIMP, si deve presumere che esso sia applicabile anche in base al diritto nazionale. L'art. 27 cpv. 4 lett. b CCC semplifica semmai la motivazione del rifiuto. Rientra nella riserva dell'*ordine pubblico* anche la mancata garanzia di standard elementari di protezione dei dati, per i quali occorre tuttavia porre requisiti elevati. L'assistenza giudiziaria dovrebbe essere subordinata in via prioritaria alla garanzia di tali standard.

2. Rinvio dell'assistenza giudiziaria (cpv. 5)

L'art. 20 cpv. 5 consente allo Stato richiesto, ossia all'autorità competente, di 20 rinviare l'esecuzione della domanda di assistenza giudiziaria e quindi di derogare al **principio della rapida esecuzione** sancito dall'art. 25 cpv. 1 CCC, dal preambolo della Convenzione e dalla possibilità di una procedura d'urgenza ai sensi dell'art. 27 cpv. 9 CCC. Ne consegue che, in assenza dei presupposti di cui al cpv. 5, la richiesta deve essere eseguita entro un termine utile. Trattandosi di un mezzo di rifiuto meno severo, non è prevista una durata massima fissa. L'esecuzione della richiesta può invece essere rinviata fintantoché sussistono i presupposti di cui al cpv. 5.

Il presupposto per il rinvio è il pericolo che l'esecuzione immediata 21 comprometta le indagini o i procedimenti penali dello Stato richiesto. Non si considera compromissione solo l'ostacolo alle indagini, ad esempio in caso di indagini segrete di lunga durata da parte dello Stato richiedente. Il rifiuto è giustificato piuttosto dal **ritardo che si verificherebbe altrimenti nell'assunzione di prove imminenti** a causa della consegna degli elementi di prova allo Stato richiedente. Tuttavia, nell'interesse di un'assistenza giudiziaria completa e rapida, si dovrebbe ricorrere con cautela alla possibilità prevista dal cpv. 5.

- 22 Secondo la sistematica dell'articolo 27 CCC, il **rifiuto e il rinvio**, a causa dei loro presupposti e delle loro conseguenze giuridiche diversi, sono indipendenti l'uno dall'altro, cosicché la decisione sul rifiuto potrebbe essere rinviata fino alla scadenza del termine di cui al cpv. 5. Una valutazione complessiva deve tuttavia essere effettuata in ogni caso al momento della decisione ai sensi del cpv. 6 e dovrebbe del resto corrispondere al principio dell'efficacia dell'assistenza giudiziaria.

3. Condizione come presupposto per il rifiuto e il rinvio (cpv. 6)

- 23 Il cpv. 6 realizza il principio dell'assistenza giudiziaria effettiva e completa ai sensi dell'art. 25 cpv. 1 CCC. Lo Stato richiedente non deve essere costretto a elaborare in modo dettagliato richieste principali e subordinate. Spetta piuttosto allo Stato richiesto **accogliere la richiesta nella misura del possibile e, in caso di riserve, consultare lo Stato richiedente**. Ne consegue innanzitutto la limitazione delle obiezioni alle parti separabili della richiesta, nella misura del possibile. La parte non interessata deve essere trattata senza indugio. Come seconda possibilità per garantire un'esecuzione tempestiva, il cpv. 6 prevede l'esecuzione a determinate condizioni. Queste condizioni riguardano in primo luogo l'utilizzo degli elementi di prova trasmessi nello Stato richiedente. Prima della consegna devono essere ottenute le relative garanzie. Spesso, ad esempio, è prevista la condizione che gli elementi di prova possano essere utilizzati solo per il procedimento in corso e non per altri procedimenti. Se, invece, sussistono dubbi sulla legittimità dell'esecuzione nello Stato richiedente, nell'ambito della consultazione si deve cercare di ottenere un'adeguamento della richiesta. Se ciò non avviene, la richiesta deve essere respinta in tutto o in parte oppure si procede secondo il cpv. 3. Anche dei diritti dello Stato richiesto ai sensi del cpv. 6 si dovrebbe fare uso con riserva nell'interesse di un'efficace assistenza giudiziaria.

D. Obblighi di comunicazione (cpv. 7)

- 24 Il cpv. 7 contiene gli obblighi di comunicazione relativi ai risultati dell'esecuzione e ai motivi di un rifiuto o di un rinvio. Ciò serve a informare lo Stato richiedente affinché possa formulare in modo più mirato **future richieste** allo stesso Stato. Non è necessaria una comunicazione separata dei motivi di una condizione. Si presume evidentemente che i motivi siano

sufficientemente evidenti dalla condizione stessa o che siano discussi con lo Stato richiedente nell'ambito di una consultazione ai sensi del cpv. 6.

E. Riservatezza (cpv. 8)

Il cpv. 8, che va oltre il cpv. 3, consente di imporre condizioni per l'esecuzione della richiesta che non servono all'utilizzabilità nello Stato richiedente, ma ad altri **interessi investigativi o politici**. La formulazione «soweit die Erledigung des Ersuchens nichts anderes gebietet» nella traduzione tedesca è ambigua: dalla versione inglese («except to the extent necessary») e francese («sauf dans la mesure nécessaire») risulta che questa parte della frase precisa il concetto di riservatezza e non limita in linea di principio la possibilità di procedere ai sensi del cpv. 8. Ai sensi del cpv. 8 è riservata in particolare anche una misura che deve necessariamente essere comunicata alla persona interessata, ad esempio alla banca dell'imputato. 25

Alla luce della formulazione restrittiva e dell'imperativo di un'assistenza giudiziaria il più possibile completa, non è possibile invocare carenze strutturali effettive, quali ad esempio problemi di corruzione all'interno delle autorità competenti, per giustificare l'impossibilità di fornire assistenza. L'eccezione dovrebbe piuttosto essere interpretata in conformità al cpv. 3, seconda parte, e riguardare quindi **ostacoli giuridici**. La riservatezza non può quindi essere garantita se le misure oggetto della richiesta, compreso il fatto che esse si basano su una richiesta di assistenza giudiziaria, devono essere rese pubbliche in base al diritto nazionale imperativo. 26

L'interesse dello Stato richiedente è solitamente quello di impedire che l'**imputato** ne venga a conoscenza. Lo stesso vale per la persona **interessata** dalla misura, purché essa sia vicina all'imputato e la misura possa in linea di principio essere eseguita in modo segreto. La riservatezza non è in ogni caso garantita se vi è una comunicazione diretta all'imputato o se è prevedibile che l'informazione giunga a conoscenza dell'interessato. Inoltre, la riservatezza non è naturalmente garantita se il fatto che è stata presentata una richiesta o il contenuto di tale richiesta diventano di dominio pubblico, ossia di una pluralità indeterminata di persone che non sono collegate tra loro da caratteristiche particolari. 27

Ciò è in contrasto con il diritto della persona interessata dalla misura a una **tutela giuridica effettiva**: se i risultati della misura vengono trasmessi a uno 28

Stato estero non vincolato dal diritto svizzero, le conseguenze di una violazione dell'AIMP non possono più essere eliminate. I diritti umani dell'imputato e della persona interessata devono essere conciliati con i legittimi interessi alla riservatezza dello Stato richiedente. La ponderazione degli interessi operata dall'AIMP è da considerarsi tendenzialmente favorevole alle persone interessate.

- 29 L'articolo 80m AIMP disciplina la notifica delle decisioni dell'autorità di esecuzione e presuppone quindi la **notifica sia della decisione di entrata in materia che della decisione finale**, nonché di eventuali decisioni intermedie. Il momento della notifica non è regolamentato. Viceversa, l'art. 63 cpv. 2 AIMP prevede misure di assistenza giudiziaria di minore entità che sarebbero vanificate da un annuncio preventivo. Ciò riguarda in particolare la perquisizione di persone e locali. Inoltre, oggetto della tutela giuridica e quindi punto di riferimento prioritario del diritto di essere sentiti ai sensi dell'art. 12 AIMP in combinato disposto con l'art. 29 PA non è la decisione di entrata in materia, bensì, ai sensi dell'art. 80e cpv. 1 AIMP, la decisione finale. È quindi ammissibile che la decisione di entrata in materia sia notificata all'interessato solo insieme alla decisione finale.
- 30 In questo modo, per le misure che per loro natura non possono essere portate a conoscenza dell'interessato – come ad esempio l'audizione –, è garantita temporaneamente la riservatezza dell'esistenza e del contenuto della richiesta. Prima di trasmettere i risultati della misura allo Stato richiedente, occorre tuttavia attendere l'**esecutività della decisione finale** ai sensi dell'art. 80d in combinato disposto con l'art. 80l cpv. 1 AIMP. Una trasmissione anticipata, che garantisce la riservatezza nei confronti dell'interessato a lungo termine, è possibile solo alle condizioni estremamente restrittive di cui all'art. 80d^{bis} AIMP, che presuppone in particolare un caso di criminalità organizzata o di terrorismo. In tal caso, la comunicazione alla persona interessata è rinviata ai sensi dell'art. 80d^{bis} cpv. 5 AIMP, ma deve essere effettuata successivamente. Non è quindi possibile garantire in alcun caso la completa riservatezza nei confronti dell'interessato circa l'esistenza di una richiesta.
- 31 Se l'interessato viene a conoscenza della misura – mediante notifica di una decisione o in altro modo – gli spettano i diritti di cui all'art. 80b cpv. 1 AIMP, vale a dire il **diritto di consultare il fascicolo** e il diritto di **partecipare agli atti d'esecuzione**. Ciò compromette la riservatezza del contenuto della

richiesta di assistenza giudiziaria. A questo proposito, tuttavia, l'art. 80b cpv. 2 lett. a e b AIMP offre un'ampia possibilità di accogliere la richiesta di riservatezza sul contenuto della richiesta.

Ai sensi dell'art. 80n cpv. 1 AIMP, l'interessato ha inoltre il diritto di **informare** il proprio mandante o cliente, di norma l'imputato, in merito alla misura di assistenza giudiziaria. La riservatezza non può quindi più essere garantita nemmeno nei confronti di quest'ultimo. L'art. 80n cpv. 1 seconda parte AIMP consente tuttavia all'autorità competente di vietare, sotto pena di sanzioni penali, l'informazione del cliente, come avviene in parte nel caso di decisioni di produzione di documenti nei confronti delle banche (art. 73 cpv. 2 CPP in combinato disposto con l'art. 292 CP). In tal modo la riservatezza è garantita almeno dal punto di vista giuridico.

La riservatezza può essere garantita in alcuni aspetti grazie a diverse norme particolari. Non esiste invece una norma generale che consenta di trattare le richieste di assistenza giudiziaria in modo riservato con la stessa efficacia delle misure interne. È discutibile se ciò soddisfi in ogni caso il **mandato di adeguamento dell'art. 25 cpv. 2 CCC**.

La seconda frase lascia allo Stato richiedente la competenza decisionale in merito al trattamento non riservato delle richieste qualora lo Stato richiesto non possa garantire la riservatezza.

F. «Procedura accelerata» (cpv. 9)

Il cpv. 9 prevede che in «casi urgenti» le richieste siano trasmesse senza la partecipazione diretta delle autorità centrali ai sensi del cpv. 2. La comunicazione avviene direttamente tra le autorità esecutive (lett. a e d) o tramite Interpol (lett. b). La Svizzera ha tuttavia fatto uso della possibilità prevista alla lett. e e ha stabilito che le richieste in arrivo devono essere indirizzate – conformemente al testo della convenzione «per motivi di efficienza» – **esclusivamente all'autorità centrale**, ossia all'Ufficio federale di giustizia. In questo modo le autorità esecutive in Svizzera non sono tenute a trattare immediatamente le richieste in arrivo. Per gli Stati richiedenti si semplifica la procedura (solo) nella misura in cui non devono comunicare tramite la loro autorità centrale. Un'autorità estera subordinata può infatti rivolgere una richiesta all'Ufficio federale di giustizia oppure la richiesta può essere trasmessa a quest'ultimo tramite Interpol.

- 36 Lo scopo dell'art. 27 CCC è quello di stabilire tra gli Stati contraenti una procedura minima che vada oltre l'assistenza giudiziaria non convenzionale. In nessun caso lo Stato richiedente deve essere trattato in modo meno favorevole rispetto a una procedura secondo l'AIMP nazionale. Le richieste ai sensi dell'art. 27 CCC possono quindi essere presentate anche attraverso i **canali di comunicazione dell'art. 29 AIMP**. Ciò comprende una procedura ai sensi dell'art. 29 cpv. 2, seconda alternativa, AIMP, secondo cui la richiesta non può essere indirizzata direttamente all'autorità subordinata, ma può essere trasmessa in copia all'Ufficio federale di giustizia almeno contemporaneamente alla richiesta.
- 37 Il cpv. 9 lett. e non contiene **alcuna riserva di reciprocità**. Le autorità svizzere subordinate possono quindi trasmettere le richieste provenienti dalla CCC direttamente alle autorità subordinate di altri Stati, a condizione che questi ultimi non abbiano fatto una dichiarazione ai sensi del cpv. 9 lett. e. Ciò non corrisponde tuttavia alla prassi abituale in Svizzera (fatto salvo il campo di applicazione delle disposizioni dei trattati internazionali).

IV. TUTELA GIURIDICA

- 38 Per il cittadino interessato dalle misure oggetto della richiesta, le possibilità di tutela giuridica sono disciplinate dall'art. 25 cpv. 4 CCC e dal **diritto nazionale dello Stato** richiesto. Se la richiesta è rivolta alla Svizzera, ai sensi dell'art. 21 AIMP può essere nominato un patrocinatore legale e contro la decisione finale può essere presentato ricorso ai sensi dell'art. 80e AIMP. Se la Svizzera richiede assistenza giudiziaria a un altro Stato, la tutela giuridica contro le misure in quanto tali è disciplinata dal diritto procedurale di quest'ultimo. Contro la richiesta svizzera, la persona interessata può presentare ricorso solo alle condizioni di cui all'art. 25 cpv. 2 AIMP, che non sussistono nel campo di applicazione dell'art. 27 CCC.
- 39 Tra lo Stato richiedente e lo Stato richiesto, l'art. 27 CCC è vincolante e, se sussistono i presupposti, crea un **obbligo di eseguire la richiesta di assistenza giudiziaria**. L'esecuzione avviene in conformità all'articolo 45 CCC, che prevede in via prioritaria una soluzione a livello diplomatico e, in subordine, la decisione da parte di un organo giurisdizionale da designare dalle parti, vale a dire il Comitato europeo per i problemi criminali (CDPC), un tribunale arbitrale o la Corte internazionale di giustizia.

BIBLIOGRAFIA

Dangubic Miro, Kommentierung zu Art. 25 CCC, in: Graf Damian K. (Hrsg.), Onlinekommentar, Übereinkommen über die Cyberkriminalität (Cybercrime Convention), abrufbar unter <https://onlinekommentar.ch/de/kommentare/ccc25>, besucht am 5.4.2024.

Dangubic Miro/Stelzer-Wieckowska Marta, Kommentierung zu Art. 80b IRSG, in: Staffler Lukas/Glassey Maria Ludwiczak (Hrsg.), Onlinekommentar zum Bundesgesetz über internationale Rechtshilfe in Strafsachen, abrufbar unter <https://onlinekommentar.ch/de/kommentare/irsg80b>, besucht am 27.2.2025.

Donatsch Andreas/Heimgartner Stefan/Simonek Madeleine, Internationale Rechtshilfe, 3. Aufl., Zürich 2024.

Gercke Marco, Kommentierung zum Übereinkommen über die Cyberkriminalität, in: Grützner Heinrich/Pötz Paul-Günther/Kress Claus/Gazeas Nikolaos/Brodowski Dominik, Internationaler Rechtshilfeverkehr in Strafsachen, 3. Aufl., Heidelberg 2022 (zit. Grützner/Pötz/Kress/Gazeas/Brodowski-Gercke).

Gless Sabine, Überblick über die Rechtshilfe in Strafsachen, in: Schomburg Wolfgang/Lagodny Otto, Internationale Rechtshilfe in Strafsachen, 6. Aufl., München 2020 (zit. Schomburg/Lagodny-Gless).

Heimgartner Stefan/Niggli Marcel Alexander, Kommentierung zu Art. 80b IRSG, in: Niggli Marcel Alexander/Heimgartner Stefan, Basler Kommentar Internationales Strafrecht, Basel 2015 (zit. BSK-Heimgartner/Niggli).

Meyer Frank, Ergänzende Kommentierung Schweiz, in: Ambos Kai/König Stefan/Rackow Peter, Rechtshilfe in Strafsachen, 2. Aufl., Baden-Baden 2020 (zit. Ambos/König/Rackow-Meyer).

Popp Peter, Grundzüge der internationalen Rechtshilfe in Strafsachen, Basel 2001.

Trautmann Sebastian, Kommentierung zu Art. 27 CCC, in: Schomburg Wolfgang/Lagodny Otto, Internationale Rechtshilfe in Strafsachen, 6. Aufl., München 2020 (zit. Schomburg/Lagodny-Trautmann).

I MATERIALI

Botschaft über die Genehmigung und die Umsetzung des Übereinkommens des Europarates über die Cyberkriminalität vom 18.6.2010, BBl 2010 4697 ff., abrufbar unter <https://www.admin.ch/opc/de/federal-gazette/2010/4697.pdf>, besucht am 5.4.2024 (zit. Botschaft 2010).

Explanatory Report to the Convention on Cybercrime, European Treaty Series – No. 185, Budapest, 23.XI.2001, abrufbar unter <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cce5b>, besucht am 5.4.2024 (zit. Explanatory Report).

ATTENZIONE: Questa versione del commentario è una traduzione automatica dell'originale. Il commentario originale è in tedesco. La traduzione è stata effettuata con www.deepl.com. Solo la versione originale fa fede. La forma tradotta del commentario non può essere citata

COMMENTO SU

Art. 28 CCC (Convenzione sulla cibercriminalità [Cybercrime Convention])

Un commentario di Julian Mausbach

CITAZIONE SUGGERITA

Julian Mausbach, Commentary of art. 28 CCC, in: Damian K. Graf (ed.), Online Commentary of the Convention on Cybercrime

Breve citazione: OK-Mausbach, art. 28 CCC N. XXX.

Art. 28 Confidenzialità e limitazioni di utilizzo

¹ Se tra la Parte richiedente e la Parte richiesta non sono in vigore trattati di assistenza giudiziaria o accordi fondati su normative uniformi o reciproche, si applicano le disposizioni del presente articolo. Tali disposizioni non si applicano, invece, qualora vi sia un trattato, un accordo o una normativa simile in vigore, a meno che le Parti interessate non decidano di applicare al loro posto i paragrafi 2–4 in tutto o in parte.

² La Parte richiesta può subordinare la trasmissione di informazioni o documenti in risposta a una domanda alle seguenti condizioni:

a. devono essere mantenuti confidenziali, se ciò è indispensabile all'esecuzione della domanda di assistenza giudiziaria; o

b. non possono essere utilizzati per indagini o procedimenti diversi da quelli indicati nella domanda.

³ Qualora la Parte richiedente non possa soddisfare una delle condizioni previste dal paragrafo 2, ne informa prontamente l'altra Parte, che decide se l'informazione vada comunque trasmessa. Se la Parte richiedente accetta la condizione, deve attenersi.

⁴ Le Parti che forniscono informazioni o documenti soggetti a una delle condizioni previste dal paragrafo 2 possono, in relazione a tale condizione, chiedere all'altra Parte precisazioni sull'uso fatto di tali informazioni o documenti.

STRUTTURA

I. Orientamento	214
II. Ambito di applicazione (art. 28 cpv. 1).....	215
III. Condizioni restrittive (art. 28 cpv. 2)	216
IV. Impossibilità di soddisfare le condizioni (art. 28 cpv. 3)	217
V. Informazioni sull'utilizzo (art. 28 cpv. 4)	217
I materiali.....	218

I. ORIENTAMENTO

1 L'articolo

28 mira a garantire l'assistenza giudiziaria, concedendo al contempo **restrizioni all'uso delle informazioni o del materiale**. In tal modo, la parte richiesta è messa in grado di fornire informazioni o materiale particolarmente sensibili solo a determinate condizioni. Tale protezione può consistere nel limitare l'uso delle informazioni allo scopo per cui è stata concessa l'assistenza o nel definire la cerchia dei destinatari, stabilendo che le informazioni o il materiale forniti non possono essere diffusi al di fuori delle autorità di polizia giudiziaria della parte richiedente. In questo senso, l'articolo 28 va inteso come una norma di mediazione classica, che da un lato è vincolata allo scopo fondamentale dell'assistenza giudiziaria e dall'altro agli interessi legittimi alla protezione (dei dati) delle informazioni e dei materiali in questione.

2 L'approccio di mediazione è garantito dal fatto che l'articolo 28 prevede un **obbligo di riservatezza**. Secondo tale disposizione, l'autorità ricevente è tenuta a trattare in modo riservato le informazioni ricevute da un altro Stato. Ciò significa che le informazioni non possono essere rese pubbliche o trasmesse a terzi non autorizzati.

3 Esiste inoltre il **principio della destinazione specifica**. In base a tale principio, lo Stato ricevente può utilizzare le informazioni solo per gli scopi per cui sono state originariamente trasmesse. Ciò significa che le informazioni non possono essere utilizzate per altri scopi o in altri procedimenti senza il consenso dello Stato che le ha trasmesse.

4 A ciò si aggiunge il fatto che anche le **deroghe alla destinazione specifica** sono soggette al consenso. Se lo Stato ricevente intende utilizzare le informazioni per scopi diversi da quelli previsti dalla destinazione, deve ottenere il consenso dello Stato che le ha trasmesse. Si garantisce così che il controllo sull'utilizzo delle informazioni rimanga nelle mani dello Stato che le ha originariamente fornite.

5 L'articolo 28 può quindi essere considerato un elemento centrale della cooperazione internazionale nella lotta contro la criminalità informatica. Esso garantisce che le informazioni scambiate tra Stati siano trattate in modo confidenziale e utilizzate solo per lo scopo previsto. L'articolo 28 crea quindi

una base per lo scambio internazionale di informazioni in un clima di fiducia e sostiene il rispetto delle norme nazionali e internazionali in materia di protezione dei dati.

II. AMBITO DI APPLICAZIONE (ART. 28 CPV. 1)

L'art. 28 si applica solo se **non esiste alcun trattato di assistenza giudiziaria** o accordo basato su norme uniformi o reciproche tra la parte richiedente e la parte richiesta. Gli accordi e i trattati di assistenza giudiziaria esistenti, con particolare riferimento all'assunzione di prove, in particolare la Convenzione dell'8 novembre 1990 relativa al riciclaggio, all'identificazione, al sequestro e al confiscazione dei proventi di attività criminali, la Convenzione europea del 20 aprile 1959 relativa all'assistenza giudiziaria in materia penale o il Secondo protocollo aggiuntivo dell'8 novembre 2001 alla Convenzione europea sull'assistenza giudiziaria in materia penale devono essere osservati ai sensi del cpv. 1 e comportano che l'art. 28 sia sostituito da questi ultimi in non pochi procedimenti di assistenza giudiziaria. 6

Se è in vigore un tale trattato o accordo, le disposizioni in materia di riservatezza e di limitazioni dell'uso sostituiscono l'art. 28. Ciò vale in ogni caso, a meno che le parti non abbiano espressamente convenuto l'applicazione dell'art. 28 cpv. 2-4. Per la maggior parte delle procedure di assistenza giudiziaria che coinvolgono le autorità svizzere, si presume che l'assistenza giudiziaria ai sensi del cpv. 1 sia fornita in base alle convenzioni e ai trattati di assistenza giudiziaria pertinenti. 7

Se e in che modo esista altrimenti un accordo tra la Svizzera e altri Stati non partecipanti alle convenzioni sull'assistenza giudiziaria citate, che escluda l'applicabilità dell'art. 28, stabilisca proprie norme di riservatezza o ricorra comunque all'art. 28 cpv. 2-4, deve essere verificato caso per caso in base alle specificità di ciascun Paese. A tal fine è utile consultare l'elenco dei trattati bilaterali e multilaterali in materia di assistenza giudiziaria penale redatto dall'Ufficio federale di giustizia. 8

Se esiste una regolamentazione tra le parti, si applica esclusivamente questa. 9 In questo modo, grazie alla chiara disposizione del cpv. 1, si evitano sovrapposizioni con altri trattati bilaterali e multilaterali di assistenza giudiziaria esistenti e accordi analoghi, cosicché nella pratica le autorità competenti possono attenersi alla regolamentazione consueta e non è

necessario chiarire il rapporto tra convenzioni concorrenti o addirittura contraddittorie.

III. CONDIZIONI RESTRITTIVE (ART. 28 CPV. 2)

- 10 Il cpv. 2 consente alla Parte contraente richiesta di porre due tipi di condizioni. Essa può innanzitutto fornire le informazioni o i documenti a condizione che questi rimangano **riservati** se e nella misura in cui la richiesta non possa essere soddisfatta in altro modo (lett. a; paragonabile alla riservatezza dell'identità di un informatore).
- 11 Inoltre, può essere imposta la condizione che le informazioni o i documenti trasmessi **non possano essere utilizzati per indagini o procedimenti diversi da quelli indicati nella richiesta** (lett. b).
- 12 La limitazione dell'uso delle informazioni e dei documenti trasmessi deve essere espressamente richiesta dalla parte contraente richiesta. Ciò vale anche per la condizione del trattamento riservato, come risulta già dal testo della norma, che prevede che la trasmissione sia subordinata a una condizione e che quindi si attenda un'attività da parte della parte richiesta.
- 13 Se non viene espressamente dichiarata tale condizione, la parte richiedente non è soggetta ad alcuna restrizione.
- 14 In particolare, con la seconda condizione, il principio di specialità sancito dall'articolo 67 AIMP, che riveste un'importanza fondamentale nella prassi, trova riscontro anche nell'articolo 28. Secondo tale principio, gli atti e le informazioni trasmessi non possono essere utilizzati nello Stato richiedente in procedimenti relativi a fatti per i quali l'assistenza giudiziaria non è ammessa, né per l'inchiesta né come prova. In Svizzera, tale divieto si estende anche e in particolare ai reati che, secondo la concezione svizzera, hanno carattere politico, militare o fiscale.
- 15 Nel quadro dei negoziati sulla Convenzione sulla criminalità informatica sono state riconosciute **due eccezioni** alla possibilità di limitare l'utilizzo. Queste sono quindi implicitamente contenute nelle disposizioni del capoverso e, in tal senso, sono a loro volta limitative, in quanto non comportano una restrizione dell'utilizzo.
- 16 La prima limitazione deriva dai principi giuridici fondamentali di molti Stati, che esigono che le informazioni e il materiale che costituiscono prove a

discarico di un imputato **siano comunicati alla difesa o a un'autorità giudiziaria**. Se le informazioni o il materiale forniti costituiscono tali prove, non si può prevedere né esigere una violazione dei principi giuridici fondamentali.

Analogamente, una limitazione non si estende ai **procedimenti giudiziari pubblici**. Il materiale trasmesso nell'ambito di accordi di assistenza giudiziaria e destinato ad essere utilizzato in un procedimento giudiziario che è normalmente pubblico non può essere oggetto di una restrizione di utilizzo corrispondente.

IV. IMPOSSIBILITÀ DI SODDISFARE LE CONDIZIONI (ART. 28 CPV. 3)

Il cpv. 3 stabilisce invece l'obbligo della parte richiedente di reagire immediatamente a una condizione qualora non possa soddisfarla. La parte richiedente deve comunicare **senza indugio tale circostanza alla parte richiesta**. Quest'ultima ha il diritto di verificare e decidere se intende comunque fornire le informazioni, pur essendo a conoscenza dell'impossibilità di soddisfare la condizione, quindi in ultima analisi a titolo incondizionato. A questo proposito, si potrà pretendere il rispetto dei principi dell'assistenza giudiziaria, il che, alla luce della decisione, significa che, nell'ottica della comprensibilità per la parte richiesta, essa ha il diritto di avvalersi del margine di discrezionalità di cui dispone anche in questo caso.

Se non viene comunicato immediatamente che una condizione non può essere soddisfatta, tale condizione è valida come condizione vincolante, come nel caso di un'accettazione esplicita della condizione.

V. INFORMAZIONI SULL'UTILIZZO (ART. 28 CPV. 4)

Il cpv. 4 costituisce un **livello di controllo**. La parte che trasmette le informazioni o il materiale ha la possibilità di farsi un'idea dell'utilizzo delle informazioni e dei materiali messi a disposizione in base a una condizione di cui al cpv. 2. A tal fine, la parte richiesta può esigere dalla parte contraente richiedente che fornisca indicazioni sull'utilizzo delle informazioni o dei documenti. Tali informazioni devono essere sufficientemente dettagliate e complete da consentire almeno la verifica del rispetto delle condizioni.

- 21 In definitiva, ciò non serve solo al controllo della parte richiedente, ma garantisce anche che la parte richiesta possa adempiere agli obblighi che le incombono, in particolare quello di garantire che non vi sia violazione dell'art. 67 AIMP.

I MATERIALI

Botschaft über die Genehmigung und die Umsetzung des Übereinkommens des Europarates über die Cyberkriminalität, BBl 2010 4697 ff., abrufbar unter <https://www.fedlex.admin.ch/eli/fga/2010/813/de>, zuletzt besucht am 19.2.2025 (zit. Botschaft CCC).

Explanatory Report to the Convention on Cybercrime Budapest, 23.XI.2001, <https://rm.coe.int/16800cce5b>, zuletzt besucht am 19.2.2025 (zit. Explanatory Report).

ATTENZIONE: Questa versione del commentario è una traduzione automatica dell'originale. Il commentario originale è in tedesco. La traduzione è stata effettuata con www.deepl.com. Solo la versione originale fa fede. La forma tradotta del commentario non può essere citata

COMMENTO SU

Art. 29 CCC (Convenzione sulla cybercriminalità [Cybercrime Convention])

Un commentario di Simon Bächtold

CITAZIONE SUGGERITA

Simon Bächtold, Commentario all'art. 29 CCC, in: Damian K. Graf (a cura di), Commentario online alla Convenzione sulla cybercriminalità [Cybercrime Convention]

Breve citazione: OK-Bächtold, art. 29 CCC N. XXX.

Sezione 2: Disposizioni specifiche

Titolo 1: Assistenza giudiziaria per misure provvisionali

Art. 29 Conservazione rapida di dati informatici memorizzati

¹ Una Parte può richiedere a un'altra Parte di ordinare o imporre in altro modo la conservazione rapida di dati memorizzati attraverso un sistema informatico situato sul territorio dell'altra Parte, in relazione ai quali la Parte richiedente intende presentare una domanda di assistenza

giudiziaria per la perquisizione o un accesso con metodi simili, per il sequestro o un'acquisizione con metodi simili o per la trasmissione.

² Una domanda di conservazione effettuata in base al paragrafo 1 deve specificare:

- a. l'autorità che richiede la conservazione;
- b. il reato oggetto delle indagini o del procedimento penale e una breve esposizione dei fatti;
- c. i dati informatici memorizzati da conservare e il loro nesso con il reato;
- d. tutte le informazioni utili a identificare il custode dei dati informatici memorizzati
o il luogo in cui si trova il sistema informatico;
- e. la necessità della conservazione; e
- f. che la Parte intende presentare una domanda di assistenza giudiziaria per la perquisizione o un accesso con metodi simili, per il sequestro o un'acquisizione con metodi simili o per la trasmissione dei dati informatici memorizzati.

³ Dopo aver ricevuto la domanda di un'altra Parte, la Parte richiasta adotta tutte le misure appropriate per conservare rapidamente i dati specificati in conformità con il proprio diritto nazionale. Per rispondere a una tale domanda e provvedere alla conservazione non è richiesta la doppia incriminazione.

⁴ Una Parte che richiede la doppia incriminazione come condizione per rispondere a una domanda di assistenza giudiziaria per la perquisizione o un accesso con metodi simili, per il sequestro o un'acquisizione con metodi simili o per la trasmissione di dati memorizzati può, con riferimento a reati diversi da quelli definiti in base agli articoli 2–11, riservarsi il diritto di respingere la domanda di conservazione in base al presente articolo, nel caso in cui abbia ragione di ritenere che, al momento della trasmissione, non possa essere soddisfatta la condizione della doppia incriminazione.

⁵ Inoltre, una domanda di conservazione può essere rifiutata solo se:

- a. la domanda è relativa a un reato che la Parte richiesta considera di natura politica o connesso a un reato politico; o
- b. la Parte richiesta ritiene che l'esecuzione della domanda possa pregiudicare la sua sovranità, la sua sicurezza, il suo ordine pubblico o altri suoi interessi essenziali.

⁶ Se la Parte richiesta ritiene che la semplice conservazione non sia sufficiente a garantire la disponibilità dei dati in futuro o possa compromettere la confidenzialità o pregiudicare in altro modo le indagini della Parte richiedente, ne informa prontamente l'altra Parte, che decide se la domanda vada comunque eseguita.

⁷ Tutti i dati conservati in seguito a una domanda di cui al paragrafo 1 saranno disponibili per un periodo non inferiore a 60 giorni per permettere alla Parte richiedente di presentare una domanda di perquisizione o di accesso con metodi simili, di sequestro o di acquisizione con metodi simili o di trasmissione dei dati. Ricevuta la domanda e in attesa che sulla stessa sia emanata una decisione, i dati continuano a essere conservati.

STRUTTURA

I. Introduzione	223
A. Perseguimento multinazionale e collaborativo della criminalità informatica.....	223
B. Importanza pratica e articoli correlati.....	223
II. Condizione di doppia incriminazione (art. 29 cpv. 3 e 4 CPC), esclusione del perseguimento politico (art. 29 cpv. 5 lett. a CPC) e violazione dell'ordine pubblico (art. 29 cpv. 5 lett. b CPC)	225
III. Sicurezza e raccolta di dati all'estero	226
A. Presentazione di una richiesta di sequestro conservativo.....	226
1. L'autorità richiedente (lett. a.).....	226
2. Il reato oggetto dell'indagine o del procedimento penale e una breve esposizione dei fatti (lett. b.).....	227
3. I dati informatici memorizzati da proteggere e il collegamento tra questi e il reato (lett. c.).....	227
4. Tutte le informazioni disponibili per identificare il custode dei dati informatici conservati o l'ubicazione del sistema informatico (lett. d.)	228
5. La necessità della conservazione (lett. e.) e l'intenzione della parte contraente di presentare una richiesta di assistenza giudiziaria (lett. f.).....	228
B. Inoltro e trattamento della richiesta di conservazione	228
C. Differenza dalla richiesta di informazioni	229
D. Procedimenti penali tramite rogatoria.....	230
E. Migliori prassi per le rogatorie verso gli USA.....	231
IV. Esecuzione delle richieste di sequestro da parte delle autorità svizzere.....	233
A. Procedura e responsabilità.....	233
B. Attuazione del diritto svizzero.....	233
Bibliografia	236
I Materiali	237

I. INTRODUZIONE

A. Perseguimento multinazionale e collaborativo della criminalità informatica

I criminali utilizzano **Internet** per commettere reati per due motivi principali. 1 Da un lato, per rimanere anonimi. Dall'altro, per scalare il loro modello di business criminale in modo economicamente vantaggioso, cioè per raggiungere un gran numero di potenziali vittime (in particolare le frodi informatiche). Inoltre, vi sono quei reati informatici in senso stretto che sono inconcepibili nel mondo analogico (ad esempio, hacking, attacchi DDOS, ecc.).

In linea con la natura di Internet come rete di comunicazione globale, la 2 criminalità informatica ha sempre luogo a **livello internazionale**. Di norma, i gruppi criminali organizzati operano in tutto il mondo, o almeno - dal punto di vista svizzero - in tutta Europa, e in alcuni casi solo in specifiche regioni linguistiche (ad esempio i Paesi di lingua tedesca). Ciò significa che nessuno Stato può combattere la criminalità informatica da solo. Le indagini informatiche devono quasi sempre essere condotte a livello internazionale o presentare aspetti transfrontalieri. Le indagini più ampie e complesse vengono definite procedimenti penali internazionali sulla base della divisione dei compiti. Il contrasto con il procedimento penale (svizzero) non potrebbe essere più chiaro. A causa della responsabilità primaria dei Cantoni nel perseguimento penale, in questo Paese si perdono ancora molte risorse per chiarire la giurisdizione nazionale. Un quadro nazionale della situazione dei fenomeni di criminalità informatica esiste al massimo in forma rudimentale.

Chi indaga sulla criminalità informatica al di fuori dell'ambito dei reati minori 3 non può generalmente evitare l'art. 29 del Codice penale (richiesta di conservazione / sequestro immediato dei dati).

B. Importanza pratica e articoli correlati

L'art. 29 CCC, insieme all'art. 32 lett. b CCC, è una delle disposizioni più 4 rilevanti dal punto di vista pratico della Convenzione sulla criminalità informatica, almeno dal punto di vista delle autorità di contrasto.

- 5 La richiesta di sequestro conservativo mira a risolvere il problema della volatilità dei dati elettronici, spesso conservati all'estero, ma i procedimenti di assistenza legale sono sempre molto lunghi. Dal punto di vista delle forze dell'ordine, questa situazione è aggravata dal fatto che molti Paesi non riconoscono la cosiddetta "conservazione dei dati", il che può portare alla perdita di dati rilevanti per le indagini prima ancora che possa essere presentata una richiesta di assistenza giudiziaria. Le richieste di conservazione hanno quindi lo scopo di consentire l'**acquisizione di** dati rilevanti per l'azione penale all'estero in modo rapido e semplice, in modo che lo Stato richiedente abbia il tempo di renderli disponibili attraverso i canali dell'assistenza giudiziaria.
- 6 A differenza della richiesta di informazioni ai sensi dell'art. 32 lett. b CPC, che può essere effettuata con una soglia bassa e senza svantaggi o costi per lo Stato richiedente, lo Stato richiedente, che invoca l'art. 29 CPC, è obbligato a richiedere effettivamente i dati protetti all'estero in un secondo momento tramite una **richiesta di** assistenza giudiziaria. La richiesta di assistenza giudiziaria comporta un certo impegno per la Procura richiedente, che quindi non farà richieste di conservazione a cuor leggero.
- 7 La questione della **natura giuridica** di una richiesta di conservazione si pone più volte. Ad esempio, se dopo la presentazione di una denuncia penale non è ancora chiaro se i sospetti iniziali siano sufficienti per avviare un procedimento penale (art. 309 cpv. 1 lett. a CPP). Solo in questo caso sono possibili e giustificate misure coercitive da parte del pubblico ministero. Se la richiesta di conservazione non fosse una misura coercitiva, sarebbe possibile per la polizia presentare una richiesta di conservazione di propria iniziativa, il che sarebbe positivo in termini di intenzione, perché più velocemente viene effettuata una conservazione dei dati, più è probabile che abbia successo. La questione della natura giuridica della richiesta non trova risposta nella Convenzione sulla criminalità informatica, ma è disciplinata dalla legge dello Stato richiesto (art. 25 cpv. 4 CCC). La risposta può quindi variare. In Svizzera, si sostiene che la polizia non può, in linea di principio, presentare una richiesta di conservazione senza il consenso del pubblico ministero, poiché quest'ultimo sarebbe obbligato a presentare una richiesta internazionale di assistenza giudiziaria in un secondo momento (possibile solo se è stato aperto un procedimento penale). La richiesta di conservazione immediata dei dati comporta anche un sequestro temporaneo delle registrazioni, che

costituirebbe una misura coercitiva nei procedimenti nazionali. Di fatto, una richiesta di conservazione deve essere trattata alla stregua di una **misura coercitiva in un procedimento penale**. Di conseguenza, una richiesta di conservazione deve essere ordinata dall'ufficio del pubblico ministero, la cui esecuzione può essere delegata alla polizia. Nei casi nazionali, tuttavia, il sequestro temporaneo da parte della polizia è consentito in via eccezionale se sussiste un "pericolo imminente" e il pubblico ministero non può essere informato in tempo utile (nemmeno verbalmente) (art. 263 cpv. 3 CPP). In questi casi eccezionali, la polizia può anche formulare autonomamente richieste ai sensi dell'art. 29 del Codice penale.

Va inoltre menzionato l'art. 16 della Convenzione, che impone agli Stati 8 membri di creare le condizioni legislative e organizzative necessarie affinché le richieste di conservazione provenienti da Stati esteri possano essere soddisfatte ai sensi dell'art. 29 della Convenzione. Nel corso dell'attuazione della Convenzione, la Svizzera ha deciso di non emanare alcun nuovo diritto processuale penale in materia (cfr. infra, n. 32).

II. CONDIZIONE DI DOPPIA INCRIMINAZIONE (ART. 29 CPV. 3 E 4 CPC), ESCLUSIONE DEL PERSEGUIMENTO POLITICO (ART. 29 CPV. 5 LETT. A CPC) E VIOLAZIONE DELL'ORDINE PUBBLICO (ART. 29 CPV. 5 LETT. B CPC)

La Convenzione sulla criminalità informatica si sforza di promuovere il più 9 possibile la cooperazione internazionale nel perseguimento dei reati informatici. Per questo motivo, la Convenzione stessa non prevede il requisito della doppia incriminazione, ma lascia agli Stati contraenti la facoltà di fornire assistenza se solo lo Stato richiedente incrimina un reato corrispondente (art. 29 cpv. 3 CCC). Gli Stati contraenti sono liberi di fare una riserva al momento della ratifica sul fatto che la doppia incriminazione è un requisito essenziale. In questo caso, lo Stato richiesto può rifiutare una richiesta di conservazione se è già chiaro a questo punto che i dati richiesti per la conservazione non possono essere rilasciati attraverso l'assistenza giudiziaria (art. 29 cpv. 4 CPC). Dei 70 Stati che hanno ratificato la Convenzione, 23 hanno espresso una riserva corrispondente, tra cui la Svizzera e gli Stati Uniti d'America. Poiché gli Stati Uniti e i loro Stati federati non hanno un reato penale analogo ai nostri **reati di diffamazione**, l'assistenza legale in questo ambito è sempre

esclusa e di conseguenza non viene accettata alcuna richiesta di sequestro conservativo.

- 10 A prescindere dalla questione della doppia incriminazione, la Convenzione sulla criminalità informatica esclude la richiesta di sequestro conservativo per i procedimenti penali a sfondo politico (persecuzione) (art. 29 cpv. 5 lett. a CCC), il che dovrebbe essere evidente dal punto di vista svizzero. Lo stesso vale se la parte contraente richiama ritiene che l'esecuzione della richiesta possa pregiudicare la sua sovranità, la sua sicurezza, il suo ordine pubblico o altri interessi essenziali (art. 29 cpv. 5 lett. b CPC).

III. SICUREZZA E RACCOLTA DI DATI ALL'ESTERO

- 11 Dal punto di vista della Svizzera, l'art. 29 CPC è particolarmente rilevante per la raccolta di dati informatici all'estero (cfr. infra, n. 12 e segg.). Tuttavia, l'articolo si applica anche alle richieste di Stati esteri alla Svizzera (cfr. infra, n. 31 e segg.).

A. Presentazione di una richiesta di sequestro conservativo

- 12 Il testo stesso della Convenzione fornisce istruzioni piuttosto dettagliate su come formulare una richiesta di conservazione. Sono esplicitamente menzionati i seguenti requisiti:

1. L'autorità richiedente (lett. a.)

- 13 In pratica, si tratta di solito di un **ufficio del pubblico ministero** (cfr. anche il precedente n. 7). Dal punto di vista della Convenzione, tuttavia, nulla impedisce alla polizia di presentare una richiesta di sequestro in stretta consultazione con il pubblico ministero (che dovrà poi presentare la richiesta di assistenza giudiziaria). Dal momento che l'obiettivo è quello di mettere al sicuro i dati volatili in tempo utile, questa soluzione potrebbe anche essere sensata. L'attuazione della richiesta di conservazione o la sua qualificazione giuridica dipendono dal diritto nazionale dello Stato richiesto (art. 25 cpv. 4 CPC). In molti Stati richiesti, l'attuazione della richiesta di conservazione (sequestro dei dati nel luogo di archiviazione) sarà qualificata come misura coercitiva, il che significa che spesso è necessaria una richiesta - o almeno

una (co)firma - da parte di un pubblico ministero. Nel complesso, la gestione è molto incoerente.

2. Il reato oggetto dell'indagine o del procedimento penale e una breve esposizione dei fatti (lett. b.)

Il punto è che lo Stato richiesto deve essere in grado di riconoscere se sussiste la **doppia incriminazione** (cfr. sopra, n. 9) e se la richiesta, che può anche comportare un notevole sforzo, è proporzionata (rapporto scopo/mezzi). Per i fenomeni comuni, tuttavia, una descrizione di due o tre frasi è sufficiente a soddisfare il requisito. 14

3. I dati informatici memorizzati da proteggere e il collegamento tra questi e il reato (lett. c).

È necessario motivare quali dati specifici devono essere protetti (ad es. dati di registrazione, file di log/dati di bordo o anche dati di contenuto, se possibile e ragionevolmente indicando anche i formati dei file). In particolare, però, occorre motivare *perché* questi dati hanno effettivamente un **collegamento con i** fatti che danno origine al **sospetto di reato**. Questo criterio è simile alla cosiddetta rilevanza potenziale delle prove nel contesto di una perquisizione nazionale ai sensi dell'art. 246 CPP (secondo cui "si presume" che i registri in questione contengano informazioni che possono essere sequestrate); in questo caso, i dati devono solo essere "potenzialmente rilevanti" o non apparire "palesamente inadatti". *Lespedizioni di pesca* sono disapprovate. Il criterio è preso molto sul serio ed è richiesta un'attenta giustificazione. Va ricordato che in altri Paesi l'autorità di sequestrare e/o consegnare i dati non spetta all'ufficio del pubblico ministero, ma deve essere ordinata da un tribunale per i provvedimenti obbligatori. Ad esempio, nei rapporti rilevanti per la pratica con gli Stati Uniti, il Dipartimento di Giustizia deve rivolgersi a un tribunale per ordinare la consegna dei dati di un fornitore di servizi mediante un mandato di perquisizione. A tal fine è necessaria una presentazione motivata e (a seconda delle circostanze) comprovata della connessione del reato con i documenti essenziali (in inglese). Il livello di fondatezza richiesto va ben oltre quello a cui sono abituati i pubblici ministeri svizzeri nell'ambito del diritto di procedura penale nazionale. In pratica, le autorità statunitensi consultano almeno l'autorità richiedente se il livello di 15

fondatezza della richiesta non è ancora sufficiente e offrono la possibilità di motivare la richiesta di conservazione in modo più dettagliato.

4. Tutte le informazioni disponibili per identificare il custode dei dati informatici conservati o l'ubicazione del sistema informatico (lett. d.)

- 16 Di norma, questo dovrebbe riferirsi semplicemente alla **società** a cui è assegnato lo specifico elemento di indirizzamento. Ad esempio, Google per gli indirizzi e-mail @gmail, Meta (per Facebook, Instagram e WhatsApp) ecc.

5. La necessità della conservazione (lett. e.) e l'intenzione della parte contraente di presentare una richiesta di assistenza giudiziaria (lett. f.).

- 17 La richiesta deve indicare esplicitamente che la richiesta è **necessaria** (in termini di sussidiarietà e proporzionalità) e deve essere confermata la volontà dell'autorità richiedente di dare seguito alla richiesta di conservazione mediante una richiesta di assistenza giudiziaria.

B. Inoltro e trattamento della richiesta di conservazione

- 18 A prescindere dalla formulazione della Convenzione sulla criminalità informatica, nella pratica esistono **due modi in** cui una richiesta di conservazione può o deve essere presentata. La via tipica è quella della rete 24/7, conformemente al testo della Convenzione (art. 35 CCC). Ogni Stato firmatario si è impegnato a gestire un punto di contatto pronto a ricevere le richieste di conservazione 24 ore su 24, sette giorni su sette. In Svizzera, questo ruolo è assunto dall'Ufficio federale di giustizia insieme all'Ufficio federale di polizia (fedpol).
- 19 Per ragioni di efficienza (evitare interruzioni dei media, automazione), tuttavia, molti grandi fornitori di servizi di comunicazione basati su Internet hanno iniziato a gestire i propri Law Enforcement Request Systems (LERS), che le autorità preposte all'applicazione della legge possono utilizzare per registrare direttamente le loro richieste in modo standardizzato e seguirne l'avanzamento senza dover coinvolgere altre autorità statali (ad esempio, l'Ufficio federale di giustizia / il Dipartimento di giustizia). È sensato, ed è stato implementato in alcuni cantoni, che un ufficio centrale presso la polizia o la procura gestisca l'accesso a tutti i **portali LERS** disponibili e presenti e gestisca le richieste di conservazione e di informazioni per conto della

direzione del caso. In questo modo, l'esperienza acquisita nel trattare con i vari fornitori di servizi può essere raccolta e analizzata a livello centrale e i case manager hanno contatti competenti per discutere in anticipo le prospettive di successo delle relative richieste.

In alternativa, le autorità di polizia possono inviare le loro richieste all'**Ufficio federale di polizia** (fedpol) via e-mail (crittografata e autenticata). Qui le richieste vengono verificate, se necessario integrate con domande, tradotte e inoltrate all'autorità competente all'estero. L'inglese è generalmente consigliato come lingua per le richieste di conservazione in tutto il mondo. Al centro di coordinamento fedpol si può anche chiedere se altre autorità di polizia svizzere hanno già presentato la stessa richiesta di conservazione, il che può fornire informazioni preziose per quanto riguarda il coordinamento delle indagini in corso (o la possibilità di presentare una richiesta di giurisdizione all'altro Cantone).

C. Differenza dalla richiesta di informazioni

Qual è la differenza tra una richiesta di sequestro conservativo e una richiesta di informazioni ai sensi dell'art. 32 lett. b CPC? A questo proposito, occorre innanzitutto fare riferimento al commento all'art. 32 CPC. In breve, la richiesta di informazioni comporta la **divulgazione volontaria** di dati a uno Stato partner del CCC direttamente da parte del fornitore di servizi. In pratica, la "volontarietà" si riferisce al fornitore di servizi e solo indirettamente all'utente/cliente del servizio. Gli utenti stabiliscono regolarmente nei loro termini di utilizzo che i dati possono essere trasmessi alle autorità di polizia; in casi specifici, i clienti interessati non vengono più interpellati. La volontarietà degli utenti è relativa, in quanto molti servizi non possono essere utilizzati senza il consenso alle condizioni d'uso (e quindi alla trasmissione dei dati alle forze dell'ordine).

Sebbene la Convenzione sulla criminalità informatica non riconosca questa restrizione, secondo il diritto nazionale degli Stati partner interessati, una richiesta di informazioni può generalmente includere solo i dati di registrazione (anche "informazioni sull'abbonato") ai sensi dell'art. 18 cpv. 3 lett. b del Codice penale (ad esempio nome, data di nascita, indirizzo, nome utente, indirizzo di fatturazione, indirizzi e-mail, indirizzo IP al momento della registrazione) e i dati marginali ("dati sul traffico", ad esempio la cronologia IP), ma generalmente **nessun** dato sul contenuto. Il termine "dati

sul contenuto" si riferisce al contenuto di una comunicazione, ad esempio un messaggio, un post, file multimediali, ecc. I dati di registrazione sono di gran lunga i più frequentemente chiariti. Le richieste di informazioni e di conservazione sono spesso presentate contemporaneamente, poiché non si sa quali dati il fornitore di servizi fornirà volontariamente.

- 23 In pratica, le richieste di informazioni vengono effettuate a una soglia molto più bassa, perché ciò non obbliga la Procura a presentare una richiesta di assistenza giudiziaria. Tale richiesta non è necessaria nemmeno perché la divulgazione dei dati è volontaria e la risposta viene fornita direttamente dal fornitore di servizi. La **disponibilità** dei fornitori di servizi a collaborare dipende in larga misura dal tipo di reato. I servizi sono regolarmente particolarmente disposti a collaborare in caso di reati sessuali, soprattutto quelli che coinvolgono i minori. I reati contro la proprietà sono più problematici. All'estremità inferiore della scala ci sono i reati di diffamazione, dove la cooperazione fallisce regolarmente a causa del requisito della doppia incriminazione (si veda sopra, n. 9 e n. 14).

D. Procedimenti penali tramite rogatoria

- 24 Come già detto più volte ed esplicitamente indicato nel testo della Convenzione, con la richiesta di sequestro il pubblico ministero si impegna a richiedere i dati sequestrati attraverso l'assistenza giudiziaria. Non mancano certo i casi in cui successivamente si scopre che i dati inizialmente sequestrati sono diventati obsoleti. Inoltre, non vi sono conseguenze dirette della **mancata richiesta di** assistenza legale reciproca (ad esempio, non vi sono implicazioni di costo). Tuttavia, in generale ci si aspetta che le procure rispettino questo obbligo previsto dal diritto della Convenzione, per non mettere a repentaglio la buona cooperazione tra gli Stati della Convenzione.
- 25 I dati sono congelati per **almeno 60 giorni** (cfr. art. 29 cpv. 7 CPC). La durata specifica è specificata nella conferma scritta della richiesta di conservazione e di solito è più lunga. Di solito l'autorità richiedente può anche richiedere una proroga del termine. La richiesta di assistenza legale deve essere presentata formalmente entro la scadenza.

E. Migliori prassi per le rogatorie verso gli USA

Data la loro grande importanza pratica, di seguito vengono illustrate le 26
migliori pratiche per le rogatorie negli Stati Uniti. Le spiegazioni che seguono
si basano sulla "Practical Guide for Requesting Electronic Evidence Across
Borders", pubblicata da UNODC, CTED e IAP, nonché sulla nostra esperienza
personale.

Le richieste di assistenza giudiziaria rivolte alle autorità straniere in casi di 27
criminalità informatica devono contenere le seguenti informazioni:

- Lingua della richiesta: le richieste di assistenza legale reciproca dovrebbero idealmente essere inserite direttamente in inglese, altrimenti dovrebbero essere tradotte;
- Fatti del caso: devono essere descritti brevemente ma in modo essenziale, indicando il luogo del reato (o del successo), l'ora esatta del reato e le modalità con cui è stato commesso;
- Eventuale modus operandi: deve essere descritto in modo dettagliato;
- Descrizione giuridica del reato, compresa la formulazione degli articoli di legge applicabili;
- Motivi della richiesta, in particolare la connessione tra il procedimento in corso e le misure richieste;
- Le prove ricercate o le azioni richieste devono essere descritte in dettaglio (ad esempio, consegna degli estratti conto relativi al conto X per il periodo da A a B, ottenimento di documenti dal provider Y da cui si possano vedere i dati di registrazione e i file di log dell'ID remoto 12345678 per il periodo tra A e B, ecc;)
- Spiegazioni relative a qualsiasi richiesta di conservazione già presentata, per cui tutti i numeri di riferimento comunicati a seguito della richiesta di conservazione devono essere elencati nella richiesta (CCIPS e numeri di riferimento di fedpol, dell'autorità di polizia straniera richiesta e della procura straniera richiesta).

Per ottenere i dati sui contenuti dai fornitori di servizi statunitensi, il 28
Dipartimento di giustizia deve ottenere un mandato di perquisizione da un
tribunale ai sensi della legge statunitense. Lo standard di prova è la "*probabile
causa*". Ciò significa che il tribunale deve essere convinto che l'account utente

in questione contenga probabilmente ancora prove rilevanti per il reato (a meno che i dati non siano già stati sequestrati provvisoriamente sulla base di una richiesta di conservazione). Inoltre, è necessaria una solida base di prove per supporre che un reato sia stato o sarà commesso e che le prove del reato si trovino nell'account utente richiesto. Le fonti di prova presentate devono essere attendibili (ad esempio, rapporti di polizia, fonti private attendibili). Devono essere fornite prove centrali. Se vengono fornite prove indiziarie, queste devono essere tradotte in inglese. In sintesi, occorre spiegare perché il titolare dell'account è l'obiettivo dell'indagine, perché si presume che l'account utente in questione appartenga a questa persona e quali prove si prevede di ottenere da questo account utente.

29 La richiesta di assistenza giudiziaria deve essere inviata per via diplomatica tramite l'Ufficio federale di giustizia oppure - se concordato e previsto - direttamente alla Procura all'estero. La guida all'assistenza giudiziaria dell'Ufficio federale di giustizia contiene informazioni più dettagliate sui canali di trasmissione specifici.

30 Nota bene:

- Per le richieste di assistenza giudiziaria in casi di criminalità informatica, è necessario indicare come base giuridica anche la CCC (a condizione che il Paese destinatario abbia ratificato la Convenzione).
- L'esposizione dei fatti, la sussunzione dei fatti nei reati e le ragioni della richiesta sono l'elemento fondamentale di una richiesta di assistenza giudiziaria internazionale.
- Informazioni dettagliate sull'assistenza giudiziaria sono disponibili nella Guida all'assistenza giudiziaria dell'Ufficio federale di giustizia, con modelli in varie lingue e un indice dei Paesi.
- Una richiesta di assistenza giudiziaria a seguito di una richiesta di sequestro conservativo deve essere presentata il prima possibile e al più tardi entro il termine di esecuzione della richiesta (art. 29 cpv. 7 CPC).

IV. ESECUZIONE DELLE RICHIESTE DI SEQUESTRO DA PARTE DELLE AUTORITÀ SVIZZERE

A. Procedura e responsabilità

Tutti gli Stati che hanno ratificato la Convenzione sulla criminalità informatica ³¹ hanno indicato quale delle loro autorità funge da punto di contatto centrale per gli Stati richiedenti ("rete 24/7", art. 35 CCC). Secondo la dichiarazione della Svizzera, si tratta principalmente dell'Ufficio federale di giustizia. Tuttavia, la Polizia giudiziaria federale (fedpol) è responsabile delle questioni relative alla Convenzione sulla criminalità informatica, in particolare delle richieste di conservazione (l'Ufficio federale di giustizia inoltra tali richieste a fedpol). Fedpol riceve circa **200 richieste** all'anno dall'estero, che a sua volta inoltra alle forze di polizia cantonali per l'elaborazione.

B. Attuazione del diritto svizzero

Il processo di elaborazione di una richiesta di sequestro conservativo ³² dall'estero in Svizzera **non è regolato dalla legge**. È notevole quanto poco il messaggio sull'attuazione della Convenzione sulla criminalità informatica si occupi di questioni procedurali e pratiche. Si limita a menzionare che gli Stati contraenti non sono obbligati a creare ulteriori strumenti giuridici oltre al sequestro e alla divulgazione.

Il diritto processuale penale svizzero **non riconosce le "ordinanze di ³³ conservazione"** ai sensi della Convenzione sulla criminalità informatica. Un ordine di conservazione sarebbe un ordine ufficiale a un fornitore di servizi di mantenere i dati disponibili per un certo periodo di tempo (tipicamente nel senso di un back-up). Poiché questo strumento non è previsto dal Codice di procedura penale, la disponibilità a lungo termine dei dati deve essere garantita in altro modo, il che può essere fatto solo attraverso un'edizione (art. 265 del Codice di procedura penale). Poiché le polizie cantonali non sono autorizzate a modificare i dati, devono trasmettere le relative richieste ricevute da fedpol alla Procura competente, che emette un ordine di edizione. Mentre il Codice di procedura penale non prevede alcuna base per gli ordini di conservazione, la conservazione dei dati prescritta dalla legge nel settore delle telecomunicazioni è stata attuata in modo simile. Sono gli stessi fornitori di servizi di telecomunicazione a dover conservare per le autorità giudiziarie i

dati di registrazione e di bordo delle comunicazioni dei loro clienti per un periodo di sei mesi (art. 21 cpv. 2, art. 22 cpv. 2 e art. 26 cpv. 5 BÜPF).

- 34 Questa formulazione svizzera della richiesta di conservazione ai sensi dell'art. 29 CPC è relativamente lontana dallo spirito della Convenzione, che prevedeva una misura rapida, non complicata e con il minor numero possibile di restrizioni per tutte le parti coinvolte. Il processo sopra descritto coinvolge almeno tre autorità e la società destinataria, ovvero numerose interfacce, il che comporta ritardi e aumenta inevitabilmente la possibilità di errori. Un ordine di divulgazione, combinato con la consegna e l'archiviazione fisica o digitale di volumi di dati, probabilmente molto consistenti, comporta anche una **notevole mole di lavoro** per i fornitori di servizi e le autorità responsabili dell'archiviazione dei dati. È in corso un dibattito internazionale per stabilire se i Paesi che non hanno introdotto ordini di conservazione ai sensi della Convenzione e si accontentano invece di ordini di divulgazione (come la Svizzera) soddisfino i requisiti della Convenzione. Sebbene la maggioranza degli intervistati sia apparentemente favorevole, vi sono ancora punti critici, in particolare per quanto riguarda gli ostacoli legali più elevati (non in Svizzera), i procedimenti più lunghi e il possibile aumento del rischio che le persone interessate vengano a conoscenza della misura, il che può vanificare lo scopo dell'indagine.
- 35 L'esecuzione di richieste di sequestro conservativo all'estero in Svizzera non fa ancora parte di un procedimento formale di assistenza giudiziaria e non è nemmeno una misura cautelare ai sensi dell'AIMP (o di altri principi del diritto dell'assistenza giudiziaria). È a monte di qualsiasi procedimento di assistenza giudiziaria. Infatti, non tutte le richieste di sequestro conservativo saranno probabilmente seguite da una richiesta formale di assistenza giudiziaria. La richiesta di conservazione trova la sua base nella stessa Convenzione sulla criminalità informatica (che è direttamente applicabile nel sistema monistico svizzero nella misura in cui è sufficientemente specifica). L'attuazione della richiesta di conservazione in questo caso non è sufficientemente specifica, motivo per cui - come già accennato - è necessario ricorrere agli istituti giuridici del diritto processuale penale nazionale, ossia il Codice di procedura penale (ad es. art. 265 CPP, edizione) nonché la Legge federale sulla polizia di transito e le sue ordinanze (ad es. art. 38 VÜPF, IR_8_IP (NAT): titolari di indirizzi IP). Il tutto sempre nell'ottica di rispettare il più possibile lo spirito della Convenzione sulla criminalità informatica (prevenzione rapida, non

complicata ed efficace della perdita di prove). Ciò significa anche che gli ordini di divulgazione emessi in esecuzione di una richiesta di conservazione devono essere accompagnati da un **divieto di** divulgazione al destinatario della divulgazione, in modo da non compromettere il successo dell'indagine (art. 29 cpv. 6 CPC; art. 73 cpv. 2 CPP in combinato disposto con l'art. 292 CPC; cfr. art. 292 CPC; cfr. art. 292 CPP; cfr. art. 292 CPC). Art. 292 CP; cfr. analogamente anche l'Art. 11b comma 2 lett. c AIMP e l'Art. 80b comma 2 lett. a AIMP). La conseguenza è che le persone interessate non sono ancora in grado di impugnare l'esecuzione stessa al momento dell'esecuzione a causa della mancanza di conoscenza. Non appena (se) viene avviata una procedura formale di assistenza legale, i proprietari dei dati (i clienti interessati del servizio) devono essere informati del loro diritto al sigillo (art. 9 AIMP in combinato disposto con l'art. 248 cpv. 2 CPP). Tuttavia, se non viene ricevuta alcuna richiesta di assistenza legale reciproca entro 60 giorni ai sensi dell'art. 29 cpv. 7 CPC e di eventuali solleciti/proroghe del termine, i dati devono essere cancellati irrevocabilmente per mancanza di una base giuridica per una conservazione più lunga.

In base alla situazione giuridica attuale, il fornitore di servizi ha il diritto di 36
sigillare i dati in quanto custode degli stessi (cfr. art. 248 cpv. 1 CPP). Tuttavia, la sigillatura da parte del **fornitore** di servizi potrebbe comportare spese inutili, in particolare nel caso in cui si debba eseguire una procedura di cancellazione che richiede molto tempo e lo Stato richiedente rinunci successivamente alla procedura di assistenza giudiziaria. Inoltre, gli interessi di riservatezza del fornitore di servizi spesso non vengono intaccati dalla divulgazione. Tuttavia, questo sarebbe un prerequisito per una richiesta di sigillo valida, in quanto il sigillo non può essere richiesto per conto di una terza parte (come il titolare del conto). D'altro canto, se i dati vengono raccolti da fornitori di servizi che, per la natura del loro servizio, dovrebbero regolarmente avere dati protetti dal segreto, ci si chiede se l'ufficio del pubblico ministero, che esegue la richiesta di conservazione (emette l'ordine di divulgazione), non debba già sigillare i dati d'ufficio al momento della divulgazione. In entrambi i casi, tuttavia, il pubblico ministero dovrebbe presentare una richiesta di dissequestro entro 20 giorni per eseguire la richiesta di sequestro (art. 248 cpv. 3 CPP), in un momento in cui il titolare dei dati non dovrebbe ancora essere a conoscenza della richiesta di sequestro e non dovrebbe quindi essere incluso nella procedura di dissequestro (a parte il fatto che di norma non ha un domicilio per le notifiche in Svizzera).

- 37 Al fine di non compromettere il successo dell'indagine e di evitare inutili tempi morti, l'unico approccio appropriato nel contesto della Convenzione sulla criminalità informatica sarebbe quindi quello di applicare il sigillo/dissequestro solo nel contesto di un procedimento formale di assistenza giudiziaria. In ogni caso, la sigillatura può essere possibile solo una volta completata la raccolta dei dati in quanto tale. Ad esempio, la raccolta di dati che si basa su un'unica richiesta di conservazione ma che richiede diverse fasi consecutive in Germania, ad esempio diverse richieste di informazioni al PTSS (prima identificazione dell'elemento di indirizzamento in base all'indirizzo IP, seconda identificazione dell'abbonato in base all'elemento di indirizzamento).
- 38 Ci si chiede se sia lecito, in base al diritto svizzero, obbligare i fornitori di servizi che non rientrano nell'ambito di applicazione del BÜPF a conservare semplicemente alcuni dati invece di consegnarli. Questo allevierebbe molti dei problemi di editing precedentemente discussi e sarebbe quindi favorevole. Tuttavia, un reale **aumento dell'efficienza** potrebbe essere ottenuto soprattutto se l'esecuzione delle richieste di conservazione estere fosse centralizzata a livello federale (fedpol), per la quale attualmente non esiste alcuna base nel Codice di procedura penale (cfr. art. 22 e segg. CPP *e contrario*). Tuttavia, una base giuridica comparabile si trova già nell'art. 18 cpv. 2 AIMP, secondo cui l'Ufficio federale di giustizia può ordinare esso stesso misure cautelari in caso di pericolo imminente.

BIBLIOGRAFIA

Bommer Felix/Goldschmid Peter, Kommentierung zu Art. 265 StPO, in: Niggli Heer/Wiprächtiger (Hrsg.), Schweizerische Strafprozessordnung, Strafprozessrecht I + II, 3. Aufl., Basel 2023.

Graf Damian K., Praxishandbuch zur Siegelung, StPO inkl. revidierter Bestimmungen – VStrR – IRSG – MStP, Bern 2022.

Thormann Oliver/Brechbühl Beat, Kommentierung zu Art. 248 StPO, in: Niggli Heer/Wiprächtiger (Hrsg.), Schweizerische Strafprozessordnung, Strafprozessrecht I + II, 3. Aufl., Basel 2023.

I MATERIALI

Botschaft über die Genehmigung und die Umsetzung des Übereinkommens des Europarates über die Cyberkriminalität vom 18.6.2010, BBl 2010 4697 ff., abrufbar unter <https://www.fedlex.admin.ch/eli/fga/2010/813/de>, besucht am 24.1.2024.

Council of Europe, The 24/7 Network established under the Convention on Cybercrime (known as the Budapest Convention), What is the 24/7 Network?, abrufbar unter: <https://www.coe.int/en/web/cybercrime/24/7-network-new->, zuletzt besucht am 24.1.2024 (zit. CoE 24/7).

Cybercrime Convention Committee (T-CY), Assessment report, Implementation of the preservation provisions of the Budapest Convention on Cybercrime, Supplementary report, 15/16.06.2015, abrufbar unter: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168044be2b>, zuletzt besucht am 24.1.2024 (zit. T-CY, Preservation Assessment).

Europarat, Cybercrime Convention Committee (T-CY), T-CY assessment report: The mutual legal assistance provisions of the Budapest Convention on Cybercrime, Strassburg, 3.12.2014, abrufbar unter: <https://rm.coe.int/16802e726c>, besucht am 17.10.2023 (zit. T-CY, Assessment Report).

Europarat, Cybercrime Convention Committee (T-CY), T-CY Cloud Evidence Group, Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY, Final report, Strassburg, 16.9.2016, abrufbar unter: <https://rm.coe.int/16806a495e>, besucht am 17.10.2023 (zit. T-CY, Cloud).

Europarat, Cybercrime Convention Committee (T-CY), The Budapest Convention on Cybercrime: benefits and impact in practice, Strassburg, 13.7.2020, abrufbar unter: <https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac>, besucht am 17.10.2023 (zit. T-CY, Benefits).

Opinion of the T-CY on the competent authority for issuing a preservation request under Articles 29 and 35 Budapest Convention, 28.11.2017, abrufbar unter: <https://rm.coe.int/t-cy-2017-18-opinion-article29-/168076cf95>, zuletzt besucht am: 19.1.2024 (zit. T-CY, Competent Authority).

Reservations and Declarations for Treaty No.185 - Convention on Cybercrime (ETS No. 185), Status as of 09/03/2024, abrufbar unter: <https://www.coe.int/en/web/conventions/full-list?module=declarations-by-treaty&numSte=185&codeNature=0>, besucht am 9.3.2024 (zit. Reservations and Declarations).

United Nations Office on Drugs and Crime (UNDOC), Sharing Electronic Resources and Laws on Crime (SHERLOC), The Practical Guide for Requesting Electronic Evidence across Borders, für Strafbehörden abrufbar unter: <https://sherloc.unodc.org/cld/en/st/evidence/practical-guide.html>, besucht am 27.09.2023, zuletzt besucht am 24.01.2024 (zit. Practical Guide for Requesting Evidence).

ATTENZIONE: Questa versione del commentario è una traduzione automatica dell'originale. Il commentario originale è in tedesco. La traduzione è stata effettuata con www.deepl.com. Solo la versione originale fa fede. La forma tradotta del commentario non può essere citata

COMMENTO SU

Art. 32 CCC (Convenzione sulla cibercriminalità [Cybercrime Convention])

Un commentario di Damian K. Graf

CITAZIONE SUGGERITA

Damian K. Graf, Kommentierung zu Art. 32 CCC, in: Damian K. Graf (Hrsg.), Onlinekommentar Übereinkommen über die Cyberkriminalität (Cybercrime Convention)

Breve citazione: OK-Graf, N. XXX zu Art. 32 CCC.

Art. 32 Accesso transfrontaliero a dati informatici memorizzati, previo consenso o quando sono pubblicamente disponibili

Una Parte può, senza l'autorizzazione di un'altra Parte:

- a. accedere a dati informatici memorizzati disponibili al pubblico (fonti aperte), indipendentemente dal luogo geografico in cui si trovano tali dati; o
- b. accedere a dati informatici memorizzati in un altro Stato o ricevere tali dati, attraverso un sistema informatico situato sul proprio territorio,

se la Parte ottiene il consenso lecito e volontario del soggetto legalmente autorizzato a trasmetterle tali dati attraverso detto sistema informatico.

STRUTTURA

I. Generale	242
A. Introduzione, storia, finalità e critica	242
B. Fondamento del diritto internazionale: principio di territorialità e sovranità (art. 31 CPC) e loro violazione (art. 32 CPC)	246
C. Materiali e interpretazione	248
D. Natura giuridica	249
E. Ambito di applicazione	249
F. Rilevanza pratica	253
II. Accesso a dati pubblicamente accessibili conservati in un altro Stato contraente ("open source") (lett. a)	254
A. Dati accessibili al pubblico	254
B. Natura giuridica: qualificazione come interferenza con i diritti fondamentali? ..	256
C. Prerequisiti per l'accesso ai dati consentito dal diritto processuale penale svizzero	258
III. Accesso ad altri dati conservati in un altro Stato contraente (lett. b)	259
A. Consenso legittimo e volontario della persona legittimamente autorizzata a divulgare i dati	259
1. Diritto alla divulgazione	259
2. Consenso	261
B. Conseguenze di un consenso legalmente valido	263
C. Presupposti per l'accesso ai dati consentito dal diritto processuale penale svizzero	264
IV. Conservazione delle prove al di là dell'art. 32 CPC secondo il principio dell'accesso	267
V. Conseguenze della violazione del diritto di sovranità straniera	271
VI. Necessità di una riforma	272
Bibliografia	273
I materiali	278

I. GENERALE

A. Introduzione, storia, finalità e critica

- 1 Dato il crescente spostamento della comunicazione verso i servizi Internet (come e-mail, social media e telefonia via Internet) e lo sviluppo tecnologico che ha spostato l'archiviazione locale verso il "cloud computing", è cambiato anche l'obiettivo investigativo delle forze dell'ordine. Il loro lavoro sta diventando sempre più complesso a causa dello spostamento delle prove nel mondo digitale. Questa complessità è dovuta, da un lato, al fatto che i dati sono di natura volatile, possono essere facilmente spostati oltre confine (cosa che può avvenire anche automaticamente, ad esempio per motivi di migliore utilizzo dei sistemi informatici) e sono accessibili alla crittografia. D'altra parte, i principali fornitori di servizi Internet (come Google, Facebook o Meta, WhatsApp, X o Microsoft), che sono diventati quasi indispensabili, operano di solito dall'estero (soprattutto dagli Stati Uniti) e da lì offrono i loro servizi a persone fisiche e giuridiche in Svizzera, mentre i dati degli utenti sono conservati all'estero. Di conseguenza, le autorità investigative devono regolarmente rivolgere la loro attenzione oltre i confini nazionali, anche nei casi nazionali. Negli Stati membri dell'UE, oltre il 50% di tutte le indagini penali prevede una richiesta transfrontaliera per ottenere dati elettronici. Ciò pone alle autorità di contrasto alcune sfide, non da ultimo di diritto internazionale, in quanto la raccolta extraterritoriale di prove costituisce a prima vista un'invasione della sovranità dell'altro Stato (cfr. infra, n. 10 e segg.).
- 2 In questo contesto transfrontaliero, le autorità devono essere dotate di poteri di intervento efficaci che consentano loro di ottenere le prove necessarie per i procedimenti penali nazionali. Nel frattempo, l'assistenza giudiziaria come meccanismo tradizionale di cooperazione internazionale è considerata inefficiente e lenta, soprattutto quando si tratta di dati volatili o che possono essere spostati, cancellati o manipolati senza particolare sforzo. Di norma, gli inquirenti non sanno in quale Stato siano archiviati i dati o, a seconda del fornitore di servizi Internet, i dati siano archiviati affatto, il che significa che al momento dell'accesso spesso non sono in grado di giudicare se stanno attraversando il "confine digitale dello Stato", né di capire in quale Stato debba essere richiesta l'assistenza giudiziaria - e anche se gli inquirenti hanno identificato uno Stato, hanno bisogno di un minimo di informazioni (ad

esempio, un account utente o un indirizzo IP) per giustificare una richiesta di assistenza giudiziaria in modo promettente. un account utente o un indirizzo IP), che a volte può rivelarsi difficile.

La necessità di una conservazione transfrontaliera delle prove era già stata 3
riconosciuta negli anni '90 e l'11.9.1995 - quando le possibilità tecniche odierne erano prevedibili solo in una certa letteratura popolare - il Consiglio d'Europa ha adottato la Raccomandazione n. R (95) 13 sui problemi del diritto processuale penale in relazione alle tecnologie dell'informazione. Il suo paragrafo 17 recita come segue: "Il potere di estendere una ricerca ad altri sistemi informatici dovrebbe essere applicabile anche quando il sistema si trova in una giurisdizione straniera, a condizione che sia necessaria un'azione immediata". Al fine di evitare possibili violazioni della sovranità dello Stato o del diritto internazionale, è necessario stabilire una base giuridica inequivocabile per tale estensione della ricerca e del sequestro. Pertanto, è urgente negoziare accordi internazionali su come, quando e in quale misura tali perquisizioni e sequestri dovrebbero essere consentiti". In attuazione di questa raccomandazione, sono stati avviati i negoziati per una convenzione sulla criminalità informatica. L'accelerazione della cooperazione internazionale e la possibile concessione di poteri transfrontalieri in violazione del principio di sovranità sono stati tra i temi centrali.

L'articolo 32 della Convenzione sulla criminalità informatica ("CCC"), che è 4
stato infine adottato, consente l'accesso ai dati memorizzati in altri Stati contraenti in due costellazioni, senza la necessità di una richiesta di assistenza legale reciproca rivolta alle autorità dell'altro Stato: da un lato, se i dati accessibili al pubblico sono interessati (lett. a), e dall'altro, se la persona autorizzata ha dato il suo consenso all'accesso (lett. b). In altre parole, l'art. 32 del Codice penale consente in questi casi un sequestro diretto dei dati conservati all'estero senza dover prima ottenere il consenso dello Stato interessato e senza dover percorrere la (difficile) strada dell'assistenza legale prima o dopo il sequestro. La zavorra amministrativa è completamente eliminata, poiché l'altro Stato non deve essere informato della raccolta di prove. Se i requisiti dell'art. 32 CP non sono soddisfatti, ossia se l'avente diritto non collabora, o se la raccolta è tecnicamente impossibile o non può essere eseguita per altri motivi, la procedura ordinaria di assistenza giudiziaria deve essere seguita come misura sussidiaria in applicazione dell'art. 31 CP, se

necessario combinata con una richiesta di conservazione immediata delle prove ai sensi dell'art. 29 CP se vi è il rischio di perdita delle prove.

- 5 Nel processo di consultazione e di legiferazione per l'attuazione del CPC in Svizzera, l'art. 32 CPC non ha dato adito a commenti, nonostante i termini utilizzati che sono aperti all'interpretazione e la relativa violazione della sovranità.
- 6 L'impostazione dell'art. 32 CDC non è rimasta esente da critiche altrove, da un lato a causa dell'abolizione della tutela dei diritti fondamentali garantiti dalla sovranità territoriale che ne consegue, senza che le autorità nazionali si rendano conto di tali violazioni dei diritti fondamentali. A questo proposito, l'art. 32 del Codice penale consente atti sovrani stranieri incontrollati sul territorio di uno Stato, che interferiscono con i diritti costituzionali delle persone interessate e di terzi, e sono sproporzionati e delicati, soprattutto per quanto riguarda gli Stati con una situazione dei diritti umani offuscata. Tuttavia, la facilitazione della raccolta di prove nei procedimenti penali associata all'art. 32 CPC è indispensabile nel perseguimento di reati con una componente digitale: le nostre vite - e quindi anche quelle degli indagati - sono diventate digitali e si svolgono sempre più in uno spazio digitale che non può essere attribuito al territorio svizzero. È vero che la maggior parte dei dispositivi elettronici oggi ha ancora una propria memoria locale, spesso generosa, che, se il dispositivo può essere sequestrato in Svizzera, può essere sequestrata, perquisita (art. 246 CPP) e confiscata (art. 263 CPP) sulla base delle regole generali di procedura penale. La tendenza, tuttavia, è quella di abbandonare l'archiviazione locale per passare a soluzioni basate su cloud o dislocate, il cui luogo di archiviazione sarà da qualche parte nel mondo, o almeno solo in parte in Svizzera (ad eccezione di settori particolari come quello bancario e della consulenza). Al giorno d'oggi le comunicazioni avvengono regolarmente anche attraverso i social media e servizi Internet analoghi, e il contenuto a volte non viene nemmeno memorizzato localmente sul proprio dispositivo. Consentendo alle autorità nazionali preposte all'applicazione della legge di uno Stato contraente di richiedere i dati direttamente ai fornitori stranieri di servizi Internet, evitando la via dell'assistenza giudiziaria (cfr. infra, nn. 48 e 55), si garantisce almeno in parte che l'accertamento sostanziale della verità nel caso di reati con una componente digitale non diventi del tutto illusorio.

D'altro canto, soprattutto gli ambienti delle forze dell'ordine considerano l'art. 32 CCC troppo restrittivo: come "minimo comune denominatore", l'art. 32 CCC rappresenta un compromesso in definitiva meno rivoluzionario. Le discussioni sull'ammissibilità della raccolta di prove transfrontaliere al di là dell'art. 32 CCC sono fallite, tuttavia, a causa della mancanza di consenso all'interno del Consiglio d'Europa. Anche nelle discussioni che sono proseguite da allora, non c'è stato in gran parte alcun consenso, sebbene la maggioranza degli Stati consideri il trasferimento delle prove al di là dei confini statali come una delle sfide centrali dell'azione penale dello Stato territoriale. Anche con il II Protocollo aggiuntivo alla Convenzione sulla criminalità informatica, adottato il 12.5.2022 e già ratificato da due Stati e firmato da altri 40 (a ottobre 2023), non è stato raggiunto un accordo. Tuttavia, deve essere consentito richiedere ai fornitori di servizi all'estero, direttamente e senza deviazioni tramite l'assistenza legale reciproca, di consegnare le informazioni di registrazione dei nomi di dominio e i dati di inventario (artt. 6 e 7 ZP II-CCC). La Svizzera non ha ancora firmato o ratificato lo ZP II-CCC, cosa che, secondo fonti dell'Ufficio federale di giustizia, non è prevista a breve - da un lato, perché la nuova normativa incide ancora una volta sul principio di sovranità, dall'altro, perché sono in corso discussioni su questo tema a livello di Nazioni Unite, che vanno attese. Infatti, le consultazioni su una Convenzione delle Nazioni Unite per contrastare l'uso delle tecnologie dell'informazione e della comunicazione a fini criminali ("Trattato delle Nazioni Unite sulla criminalità informatica") sono in fase avanzata. Tuttavia, l'attuale bozza, sostenuta dalla maggioranza, non prevede la raccolta transfrontaliera di prove, motivo per cui non sembra opportuno attendere la firma e la ratifica della ZP II-CCC.

Il Regolamento (UE) 2023/1543 sulle ordinanze europee di consegna e sulle ordinanze europee di conservazione delle prove elettroniche nei procedimenti penali e nell'esecuzione delle pene detentive a seguito di procedimenti penali del 12 luglio 2023 ("e-Evidence"), recentemente adottato, fa un passo avanti rispetto all'art. 32 del Codice penale. 2023 ("Regolamento e-Evidence"), secondo il quale le autorità giudiziarie di uno Stato membro possono richiedere prove elettroniche direttamente a un fornitore di servizi di un altro Stato membro (art. 1 cpv. 1 del Regolamento e-Evidence) e i fornitori di servizi sono legalmente obbligati a modificare i dati entro 10 giorni o il termine stabilito (art. 10 del Regolamento e-Evidence). L'art. 32 CCC, invece, si basa sulla natura volontaria dei fornitori di servizi stranieri: se non

soddisfano la richiesta o non la soddisfano completamente, deve essere intrapresa la via dell'assistenza reciproca, anche in caso di rifiuto arbitrario, opaco o immotivato di collaborare. L'art. 18 cpv. 1 lett. b CDC prevede almeno che il fornitore di servizi Internet che offre i propri servizi "sul territorio della parte contraente" debba consegnare su richiesta i dati di inventario relativi a tali servizi. Tuttavia, il Tribunale federale non ammette l'ordine di rivelare i dati a un provider straniero sulla base dell'art. 18 cpv. 1 CPC, o al massimo considera tale ordine legittimo se rivolto alla sua filiale svizzera, a condizione che quest'ultima possieda o controlli i dati.

- 9 La critica alle limitazioni dell'art. 32 CPC, che è stata espressa soprattutto negli ambienti delle forze dell'ordine, è diventata un po' più silenziosa in Svizzera. Il fatto che la comunità internazionale non abbia ancora trovato una soluzione consensuale non ha impedito al Tribunale federale (probabilmente per motivi di praticabilità, anche se in spregio al principio di sovranità) di consentire anche la raccolta transnazionale di prove dai dati senza il consenso delle persone autorizzate, con un ricorso implicito al cosiddetto principio dell'accesso (cfr. *infra*, n. 63 ss.).

B. Fondamento del diritto internazionale: principio di territorialità e sovranità (art. 31 CPC) e loro violazione (art. 32 CPC)

- 10 Il principio di territorialità rappresenta una barriera all'azione dello Stato che si sottrae alla sovranità del diritto internazionale. Non serve solo a limitare l'applicabilità del diritto penale interno a situazioni straniere - sebbene vi siano delle eccezioni - ma limita anche l'azione dello Stato al proprio territorio. Il compimento di atti ufficiali in territorio straniero non è completamente vietato. Tuttavia, a meno che tale comportamento non sia espressamente consentito da accordi internazionali (di mutua assistenza legale), da trattati bilaterali o almeno da autorizzazioni ad hoc, costituisce un'inammissibile violazione della sovranità dello Stato e può essere punito di conseguenza secondo il diritto straniero. Anche gli atti ufficiali non autorizzati in territorio straniero sono sanzionati dal diritto svizzero (art. 299 CP; cfr. anche art. 271 CP). Anche le prove raccolte in violazione del principio di territorialità non possono essere utilizzate nei procedimenti penali nazionali (cfr. *infra*, n. 69 e segg.).

In particolare, gli "atti arbitrari di coercizione e di intervento sul territorio straniero" violano la sovranità dello Stato e sono quindi contrari al diritto internazionale. Pertanto, a meno che non si ricorra all'assistenza legale dello Stato estero, l'arresto di persone all'estero da parte di funzionari svizzeri è altrettanto inammissibile quanto lo svolgimento di interrogatori, l'esecuzione di esami visivi o l'esecuzione diretta di sentenze. Secondo il Tribunale federale, lo stesso vale per l'invio di convocazioni a imputati domiciliati all'estero, che non possono essere accompagnate da minacce di coercizione, cioè devono essere semplicemente inviti. Sembra quindi chiaro che le autorità giudiziarie non possono raccogliere fisicamente prove all'estero o compiere atti processuali in loco senza passare attraverso il canale dell'assistenza legale o senza che tali atti siano esplicitamente consentiti in un accordo. Le perquisizioni domiciliari arbitrarie o il sequestro e la perquisizione di dispositivi elettronici o documenti in territorio straniero sono quindi indubbiamente vietati. 11

Non sono diverse le situazioni di raccolta delle prove in cui le autorità giudiziarie penali non sono fisicamente presenti sul territorio straniero, ma svolgono azioni investigative in Svizzera che incidono sulla sovranità territoriale straniera. Ciò include, ad esempio, l'osservazione di persone sulla sponda tedesca del Reno da parte di agenti di polizia svizzeri di Sciaffusa, così come l'interrogatorio video di un imputato all'estero da parte di un tribunale svizzero. Anche questo comportamento viola il diritto internazionale, poiché i suoi effetti sono equivalenti a un atto di sovranità direttamente sul territorio straniero. 12

Anche l'accesso a sistemi informatici all'estero da una sede in Svizzera e quindi il sequestro di dati archiviati all'estero sono da considerarsi atti di sovranità extraterritoriale. La comunità degli Stati rivendica la propria sovranità anche per quanto riguarda i sistemi di elaborazione dati situati sul proprio territorio e i dati ivi memorizzati. I poteri di ricerca nazionali non possono legittimare tali sconfinamenti nei diritti sovrani stranieri. Ciò è stato riconosciuto in linea di principio dal Tribunale federale (cfr. tuttavia infra, n. 63 e segg.) e si riflette in particolare nelle (intense) discussioni sul contenuto e sull'ulteriore sviluppo del CCC. 13

Nel momento in cui la sovranità di uno Stato straniero viene invasa in tal senso, esso deve di conseguenza acconsentire, fornendo assistenza legale su richiesta individuale o concedendo ai partner internazionali il diritto di agire 14

di conseguenza tramite un trattato o un accordo ad hoc. Esempi di cessione parziale della sovranità svizzera si possono trovare negli accordi con i Paesi limitrofi in materia di "hot pursuit" di polizia o, in misura limitata, nel contesto della Convenzione sulla criminalità informatica. La creazione dell'art. 32 CCC ha infatti eliminato la necessità di una richiesta di assistenza reciproca in due costellazioni: Da un lato, l'accesso ai dati informatici memorizzati accessibili al pubblico è consentito, indipendentemente dalla loro ubicazione geografica (lett. a). Dall'altro lato - e in modo molto esteso rispetto ad altri accordi di assistenza reciproca - secondo l'art. 32 lett. b CCC, una parte contraente può "accedere a dati informatici memorizzati situati nel territorio di un'altra parte contraente per mezzo di un sistema informatico nel suo territorio o ricevere tali dati se ottiene il consenso legittimo e volontario della persona che è legittimamente autorizzata a comunicarle i dati per mezzo di tale sistema informatico". Ciò legittima non solo la richiesta diretta ai provider stranieri di consegnare le informazioni, ma anche l'accesso delle autorità stesse attraverso gli account utente esistenti (cfr. infra, n. 55). In altre parole, il Codice penale stabilisce in termini vincolanti per gli Stati contraenti in quali circostanze le autorità possono accedere direttamente ai dati situati all'estero (cioè alle condizioni dell'art. 32 del Codice civile) e quando sono obbligate a presentare una richiesta formale di assistenza reciproca (in tutti gli altri casi; art. 31 del Codice civile). Ciò dimostra che l'accesso a dati stranieri, indipendentemente dal fatto che i membri delle autorità di polizia non siano fisicamente presenti sul territorio straniero durante tali misure di raccolta delle prove, è considerato una violazione fondamentale della sovranità. Nel corso della stesura del CCC, è emerso chiaramente che "non è stato possibile raggiungere un consenso su norme di più ampia portata in base alle quali le condizioni di accesso unilaterale da parte di uno Stato ai dati situati in un altro Stato parte possano avvenire senza l'autorizzazione di quest'ultimo".

C. Materiali e interpretazione

- 15 I termini utilizzati dall'art. 32 CDC e le costellazioni da esso contemplate sono stati solo parzialmente spiegati in modo più dettagliato nella relazione esplicativa del CDC - mutatis mutandis il "messaggio" del Consiglio d'Europa sul CDC - il che comporta il rischio che le autorità degli Stati contraenti li interpretino in modo diverso. Tuttavia, questa sembra essere una decisione deliberata. Dopotutto, un gruppo di lavoro sull'accesso transfrontaliero ai dati ("Gruppo transfrontaliero T-CY") del Comitato delle Parti ("Comitato della

Convenzione sulla criminalità informatica", "T-CY") ha pubblicato il 3.12.2014 una nota orientativa sull'accesso transfrontaliero ai dati ai sensi dell'art. 32 del TCC, che può essere utilizzata come ausilio interpretativo. Tuttavia, i presupposti dell'art. 32 CDC - come ad esempio la questione di chi sia legittimato a concedere il consenso ai sensi dell'art. 32 lett. b CDC - devono essere determinati in ultima analisi in base al diritto nazionale (cfr. infra, n. 41 e segg.); a questo proposito, una definizione nazionale e quindi possibili opinioni divergenti tra gli Stati contraenti sono inevitabili.

Secondo il Consiglio federale, la disposizione dovrebbe essere interpretata in modo restrittivo "per contrastare il pericolo di abusi che eludano l'assistenza reciproca o che violino la privacy di terzi". Tuttavia, se si tiene conto dell'effetto che l'art. 32 CPC si prefigge - l'accelerazione del procedimento o la semplificazione della raccolta delle prove - si lascia spazio a interpretazioni pratiche e praticabili. 16

D. Natura giuridica

L'art. 32 CDC è una norma di diritto internazionale "self-executing", direttamente applicabile al momento della ratifica. Le parti contraenti concedono così agli altri Stati contraenti il diritto di accedere direttamente ai dati presenti sul loro territorio, evitando il canale dell'assistenza giudiziaria. In altre parole, la disposizione prevede una "rinuncia alla procedura interna nello Stato richiesto". Le autorità giudiziarie degli Stati contraenti possono avvalersi direttamente dell'art. 32 CCC, sia nei procedimenti penali interni per legittimare la corrispondente raccolta di prove all'estero (per cui devono continuare a rispettare le norme procedurali interne, cfr. infra, n. 56) - l'art. 32 CCC non costituisce una misura coercitiva originaria a questo riguardo - sia per invocare l'assenza di interferenze illecite con la sovranità straniera in relazione allo Stato contraente interessato. In relazione all'IMAC, le disposizioni del CCC prevalgono su quelle dell'IMAC (art. 1 cpv. 1 IMAC). 17

E. Ambito di applicazione

L'art. 32 CPC consente il sequestro di dati informatici memorizzati in un altro Stato contraente. 18

Ai sensi dell'art. 1 lett. b CPC, per dati informatici si intendono tutte le rappresentazioni "di fatti, informazioni o concetti in una forma adatta 19

all'elaborazione in un sistema informatico, compreso un programma in grado di avviare l'esecuzione di una funzione da parte di un sistema informatico". L'art. 32 del Codice Civile copre quindi l'accesso ai dati di inventario, di traffico o marginali, nonché ai dati di contenuto memorizzati o in fase di trasmissione al momento dell'accesso. In virtù della loro qualificazione giuridica di dati elettronici, anche i beni crittografati, ad esempio, possono essere sequestrati in applicazione dell'art. 32 lett. b CCC, a condizione che le persone autorizzate concedano la loro autorizzazione.

- 20 L'art. 32 CCC fa esplicito riferimento al luogo di archiviazione dei dati specificamente previsti (art. 32 lett. b CCC: "[...] dati informatici archiviati situati nel territorio di un'altra Parte"; cfr. anche art. 31 CCC: "[...] archiviati per mezzo di un sistema informatico situato nel territorio della Parte richiesta"). Nel caso di dati archiviati in più luoghi, è determinante il luogo di archiviazione dell'insieme di dati che deve essere specificamente sequestrato. Di conseguenza, l'accesso in applicazione di questa disposizione è consentito solo se il CCC è applicabile nel luogo in cui i dati sono memorizzati. Poiché nessuno dei 68 Stati contraenti ha formulato una riserva all'art. 32 CCC, l'esame può limitarsi a verificare se lo Stato del luogo di conservazione da colpire è parte contraente della Convenzione sulla criminalità informatica, ossia se l'ha firmata e ratificata.
- 21 L'art. 32 CCC non è applicabile a circostanze puramente nazionali: Se i dati sono memorizzati localmente su un terminale o un server situato in Svizzera e qui protetti, si applica il diritto nazionale svizzero (in particolare l'art. 246, l'art. 263 e l'art. 265 CPP, per i dati marginali si veda l'art. 273 CPP). Ciò vale anche se le registrazioni di dati stranieri si trovano nella cache del dispositivo sequestrato qui al momento dell'accesso. Tuttavia, se il dispositivo viene utilizzato come "chiave" o "gateway" per accedere a servizi che hanno memorizzato i propri dati all'estero (ad es. cloud, webmail, ecc.) senza che questi siano memorizzati localmente sul dispositivo, si tratta di un sequestro transnazionale di dati e deve essere osservato l'art. 32 CPC (cfr. tuttavia di seguito, n. 63 e segg.). Il diritto nazionale svizzero è applicabile anche se i fornitori stranieri hanno filiali o partner svizzeri che memorizzano i dati in Svizzera. In questo caso, l'accesso può avvenire presso questi ultimi. Tuttavia, i centri dati non rientrano solitamente in questa categoria, in quanto i dati memorizzati presso di essi sono spesso criptati e difficilmente possono essere letti senza la collaborazione o la raccolta forzata dei dati presso le persone

autorizzate a riceverli. Le persone straniere devono quindi essere invitate a consegnare i dati o le chiavi in applicazione dell'art. 32 lett. b CPC o in via sussidiaria tramite l'assistenza giudiziaria. L'art. 32 lett. b CPC si applica anche se le filiali nazionali o i partner di fornitori stranieri sono invitati dal pubblico ministero a consegnare i dati che hanno memorizzato all'estero. Correttamente, a una persona nazionale non può essere ordinato, sotto minaccia di coercizione, di ottenere prove a disposizione delle autorità giudiziarie all'estero, anche se queste dovessero riguardare dati ai quali ha diritto di accedere. A questo proposito, il Tribunale federale ha ritenuto che un ordine di rivelare dati ai sensi dell'articolo 265 del CPP a una filiale svizzera di un fornitore di servizi Internet fosse ammissibile se aveva accesso ai dati in questione ed era autorizzato ad accedervi ("pouvoir de disposition, en fait et en droit, sur ces données"). Ciò non è in contrasto con quanto appena detto, in quanto l'ordine di divulgazione non costituisce ancora una misura coercitiva e può essere inteso e valutato in questo contesto come una richiesta di divulgazione volontaria ai sensi dell'art. 32 del CDC.

Per quanto riguarda i Paesi terzi che non hanno aderito alla Convenzione, si 22
deve presumere che la sovranità dello Stato vieti qualsiasi accesso online ai dati (non pubblici, cfr. infra, n. 35) e che quindi l'unica possibilità sia quella di seguire la via dell'assistenza reciproca.

È ovvio basarsi sul luogo di archiviazione, perché gli Stati possono invocare il 23
principio di sovranità anche per quanto riguarda l'infrastruttura informatica situata sul loro territorio. Tuttavia, è problematico che al momento dell'accesso, spesso non è noto né all'autorità di contrasto né alla persona autorizzata ad accedere ai dati e nemmeno al custode dei dati dove questi siano conservati in un determinato momento. Ad esempio, i fornitori di servizi Internet a volte non conservano i dati dei loro clienti nel loro paese di residenza, ma altrove. Il luogo di archiviazione può anche cambiare nel tempo a causa di ristrutturazioni tecniche o trasferimenti in altri luoghi (più economici). In ogni caso, spesso non è possibile determinare con certezza il luogo di conservazione al momento dell'accesso ai dati. Ciò solleva la questione di come affrontare il caso standard in cui l'autorità di contrasto non è in grado di determinare, al momento del sequestro previsto, se i dati sono archiviati in uno Stato contraente del CCC, in un Paese terzo o addirittura nel proprio Paese. I materiali sull'art. 32 del TCC non trattano questo aspetto in modo definitivo; la nota orientativa del T-CY si limita a prevedere che, in

situazioni in cui il luogo di archiviazione è sconosciuto o incerto, gli Stati contraenti stessi dovrebbero valutare la legittimità dell'accesso alla luce del diritto interno, dei principi di diritto internazionale pertinenti o di considerazioni sulle relazioni internazionali ("[...] le parti possono dover valutare esse stesse la legittimità di una perquisizione o di un altro tipo di accesso alla luce del diritto interno, dei principi di diritto internazionale pertinenti o di considerazioni sulle relazioni internazionali"). Nel caso di un luogo di stoccaggio sconosciuto, si suggerisce quanto segue: Se per l'applicabilità dell'art. 32 CPC fosse richiesta la conoscenza certa che il luogo di archiviazione si trova in uno Stato contraente, l'art. 32 lett. b CPC perderebbe il suo significato e il sequestro dei dati cloud sarebbe ridotto all'assurdo. "La mera possibilità di un luogo di archiviazione in un Paese terzo non può far scattare l'obbligo di fornire assistenza reciproca, soprattutto perché non è chiaro a quale Paese ci si debba rivolgere a tal fine. Chiarimenti dettagliati sul luogo di stoccaggio sono spesso impossibili prima dell'accesso o richiedono troppo tempo - è vero: se non c'è urgenza e il luogo di stoccaggio può essere determinato tecnicamente senza particolari sforzi, si dovrebbe fare uno sforzo. In considerazione dell'idea di accelerazione del CCC, tuttavia, non sarebbe consigliabile aspettare di conoscere con certezza il luogo, soprattutto se si rischia di perdere delle prove. Se a posteriori dovesse emergere che il luogo di conservazione si trovava effettivamente in un Paese terzo, sarà necessario ottenere una successiva autorizzazione per l'accesso ai dati attraverso l'assistenza giudiziaria (cfr. infra, n. 71).

- 24 Per quanto riguarda i grandi fornitori di social media, la situazione è un po' più complicata. Hanno la loro sede centrale negli Stati Uniti, ma le loro sedi europee sono spesso in Irlanda e, secondo le loro stesse informazioni (che non sono necessariamente corrette alla luce del Cloud Act statunitense), hanno accesso ai dati dei clienti europei e svizzeri solo dall'Irlanda (cosa che i provider giustificano con il Regolamento generale europeo sulla protezione dei dati del 27 aprile 2016 ["DSGVO"]), anche se i dati sono regolarmente archiviati in altri Paesi (ad esempio in Svezia). Tuttavia, l'Irlanda non ha ancora ratificato il CCC. Di conseguenza, ci si chiede se le richieste ai sensi dell'art. 32 lett. b del CDC di dati europei all'attenzione della filiale irlandese siano ammissibili e se i dati raccolti possano essere utilizzati. In alternativa, si deve considerare la Svezia come possibile luogo di archiviazione, anche se i dati possono essere accessibili lì, ma è probabile che siano criptati e quindi inutilizzabili? Oppure si dovrebbe intervenire sulla società madre americana,

che dovrebbe ottenere i dati dalla sua filiale europea? In pratica, l'esplosività di questa domanda è mitigata dal fatto che le richieste di informazioni possono essere effettuate tramite "portali per le forze dell'ordine" forniti dai fornitori di servizi Internet - da quale società del gruppo i fornitori mettano poi a disposizione delle autorità i dati richiesti o come si siano organizzati internamente dipende da loro e non è necessario esaminare ulteriormente, soprattutto perché le autorità di polizia non hanno modo di verificare dove i dati modificati siano stati effettivamente archiviati e quale società del gruppo vi abbia avuto accesso.

Alla luce di tutte queste difficoltà, il luogo di conservazione ha poco senso 25 come criterio decisivo. De lege ferenda, il criterio del luogo di conservazione dovrebbe quindi essere abbandonato per l'art. 32 del TCC ed essere invece collegato alla sede legale o al luogo di residenza della persona che ha accesso legittimo ai dati. In alternativa (in conformità al Regolamento UE sulle prove elettroniche e all'Art. 18(1)(b) del CPC), potrebbe anche essere sufficiente che la società in questione offra i propri servizi nello Stato in questione.

F. Rilevanza pratica

L'art. 32 CPC si è sviluppato come un mezzo indispensabile per perseguire i 26 reati con una componente digitale. Le autorità svizzere preposte all'applicazione della legge si avvalgono regolarmente dell'Art. 32 CCC, sia attraverso la raccolta di informazioni open source ("OSINT") in applicazione dell'Art. 32 lett. a CCC, sia attraverso l'accesso ai dati in seguito alla divulgazione volontaria dei dati di accesso da parte della persona svizzera avente diritto ai dati ai sensi dell'Art. 32 lett. b CCC o, in particolare, attraverso l'accesso ai dati in seguito alla divulgazione volontaria dei dati di accesso. b CCC o, in particolare, attraverso richieste dirette ("richieste di informazioni") a fornitori di servizi Internet esteri per la divulgazione di dati di inventario, marginali o di contenuto (in pratica, di solito vengono forniti solo dati di inventario e marginali, mentre per i dati di contenuto è necessario seguire la via dell'assistenza reciproca, se necessario in combinazione con una "richiesta di conservazione" ai sensi dell'art. 29 CCC). Le cifre relative alle richieste dirette di informazioni sono notevoli: nella prima metà del 2022, solo Google ha ricevuto oltre 422.000 richieste dirette, di cui 1.357 dalle forze dell'ordine svizzere, il 90% delle quali è stato approvato. Tuttavia, i provider non sono responsabili se rifiutano una richiesta; possono stabilire loro stessi le

condizioni di consegna, possono anche modificarle più volte e, inoltre, le condizioni variano notevolmente a seconda del provider. Ciò è accettabile nell'ambito del regime attuale, poiché l'art. 32 del Codice Civile si basa sulla volontarietà.

II. ACCESSO A DATI PUBBLICAMENTE ACCESSIBILI CONSERVATI IN UN ALTRO STATO CONTRAENTE ("OPEN SOURCE") (LETT. A)

A. Dati accessibili al pubblico

- 27 La raccolta e l'analisi di "informazioni di fonte aperta" è definita nel settore dell'intelligence come "OSINT" ("Open Source Intelligence"). L'uso di dati accessibili al pubblico si è sviluppato anche nelle forze dell'ordine come metodo investigativo utile e non invasivo. Questo è supportato dall'industria tecnologica, che ha sviluppato strumenti con i quali i dati non devono più essere raccolti manualmente, ma vengono raccolti automaticamente: Ad esempio, fornendo un software con cui è possibile estrarre tutte le informazioni pubblicamente accessibili da Facebook e visualizzarle in alberi di relazioni e sulla timeline, oppure strumenti tecnici per poter tracciare il flusso di denaro delle criptovalute (la cui blockchain è pubblicamente accessibile). Anche l'uso dell'intelligenza artificiale non è più un sogno del futuro.
- 28 I dati sono pubblici se sono liberamente accessibili attraverso un sistema di elaborazione dati e non sono sottratti all'accesso generale da speciali misure di sicurezza. È sufficiente che siano resi accessibili a una cerchia indefinita di utenti, anche se è richiesto un login, "ma questo è in linea di principio concesso a ogni utente se è stato compilato un modulo di login corrispondente". Un sistema può anche essere solo parzialmente pubblico. I dati che "possono essere consultati solo attraverso l'interfaccia di un dispositivo terminale situato nell'oggetto di ricerca - non accessibile al pubblico", invece, non sono "open source".
- 29 Esempi di dati accessibili al pubblico sono - nel senso di un elenco non esaustivo - i mezzi di comunicazione di massa liberamente accessibili (stampa [anche se protetta da un paywall], radiodiffusione), tutte le informazioni che possono essere reperite su Internet (clearnet così come darknet), le

applicazioni basate sul web (come Google Earth), le informazioni sulla blockchain accessibili al pubblico (ad esempio nel caso di Bitcoin), su Internet (ad esempio nel caso di Bitcoin), su Internet (ad esempio nel caso di Bitcoin). Bitcoin), dati pubblicamente accessibili sul sito web sotto l'indirizzo di dominio di un'azienda o di un'amministrazione, webcam liberamente accessibili, una mailing list aperta a tutti gli interessati, dati liberamente disponibili su una piattaforma di condivisione, l'attingimento di dati tecnici da un server web, la determinazione di informazioni sul dominio tramite database "WhoIs", informazioni su debitori, catasto, registro delle imprese e anagrafe dei residenti liberamente accessibili all'estero o a pagamento o atti disponibili di procedimenti penali, amministrativi e civili, osservazione di chat pubbliche, forum aperti su Internet e social network a comunicazione pubblica (utilizzo di dati pubblici, foto e relazioni su Facebook, informazioni da X, Instagram, LinkedIn ecc.)). Un post in un gruppo chiuso (forum online, Facebook o simili) può essere qualificato come pubblico anche nel caso di gruppi con un numero elevato di membri o con accesso di fatto illimitato, a meno che il gruppo di persone non sia specificamente delimitato e le persone siano personalmente collegate tra loro. Di conseguenza, "i gruppi di utenti chiusi in cui gli amministratori del sito verificano l'identità degli utenti caso per caso e un investigatore potrebbe accedere solo, ad esempio, falsificando una legenda, non possono più essere definiti pubblici".

A seconda delle circostanze, non solo i dati di contenuto (dati personali o di altro tipo), ma anche i dati di inventario (ad esempio le informazioni di registrazione da database "WhoIs") o (raramente) anche i dati marginali possono essere pubblici e quindi raccolti in applicazione dell'art. 32 lett. a CCC. 30

Ai fini della qualificazione come dati accessibili al pubblico, è irrilevante che i dati siano stati pubblicati senza autorizzazione o con il consenso della persona interessata. Se la pubblicazione è avvenuta illegalmente (ad esempio, violando gli obblighi di segretezza legale), i dati possono essere utilizzati nei procedimenti penali nazionali se possono essere ottenuti legittimamente dalle autorità giudiziarie e se la ponderazione degli interessi depone a favore del loro utilizzo. Di conseguenza, per quanto riguarda il primo criterio, è necessario chiarire se i dati avrebbero potuto essere ipoteticamente sequestrati anche se non fossero stati pubblici, ossia se avrebbero potuto 31

essere ottenuti ai sensi dell'art. 32 lett. b del Codice penale o tramite l'assistenza giudiziaria.

B. Natura giuridica: qualificazione come interferenza con i diritti fondamentali?

- 32 È discutibile fino a che punto la raccolta e l'analisi di dati accessibili al pubblico possano essere qualificate come un'interferenza con i diritti fondamentali e, di conseguenza, come una misura coercitiva ai sensi dell'art. 196 CPP. La risposta a questa domanda è fondamentale, da un lato per determinare la misura in cui è possibile accedere a dati pubblici situati in un Paese terzo, dall'altro perché, in caso di risposta affermativa, deve esistere una base giuridica sufficientemente concreta (art. 197 cpv. 1 lett. a CPP). Quest'ultima, tuttavia, è già realizzata dall'art. 95 CPP (acquisizione di dati personali).
- 33 Ai sensi dell'art. 196 CPP, le misure coercitive sono definite come atti procedurali delle autorità penali che servono, tra l'altro, ad assicurare le prove, nella misura in cui interferiscono con i diritti fondamentali delle persone interessate. L'art. 196 CPP quindi (contrariamente alla formulazione ["misura coercitiva"]) non presuppone necessariamente la coercizione, ma piuttosto si basa in modo decisivo sul fatto che la misura debba essere considerata una violazione dei diritti fondamentali delle persone interessate. Oltre al diritto alla libertà personale e alla garanzia della proprietà, è in primo piano la protezione della privacy ai sensi dell'articolo 13 della Cost. e dell'articolo 8 della CEDU, o più specificamente il diritto all'autodeterminazione informativa ivi sancito. Gli interventi su questo diritto costituzionale comprendono la sorveglianza telefonica, la raccolta di dati di telecomunicazione, il prelievo e l'analisi del DNA e delle impronte digitali, l'osservazione (compresa la sorveglianza sistematica da parte di detective privati), le registrazioni video da parte della polizia, l'uso di un IMSI catcher e le ricerche online protette da password o il sequestro di messaggi di chat.
- 34 Per quanto riguarda la sorveglianza automatizzata del traffico, la Corte Suprema Federale ha affermato che la protezione della privacy non si limita ai locali privati, ma si estende anche alla sfera pubblica privata; l'articolo 13 della Costituzione Federale copre anche le questioni di vita con contenuto personale che si verificano nella sfera pubblica. Secondo la Corte costituzionale federale tedesca, l'accesso a "contenuti di comunicazione e

informazioni disponibili su Internet che sono rivolti a tutti o almeno a un gruppo di persone non ulteriormente delimitato" non può ancora essere definito correttamente come una violazione del diritto all'autodeterminazione informativa. I contenuti riservati a un determinato gruppo di utenti su blog, forum o social media e quindi rivolti a un ambiente caratterizzato da relazioni personali o da una particolare fiducia sono da attribuire alla sfera privata ai sensi dell'art. 13 cpv. 1 Cost. e il loro accesso è da considerarsi una violazione dei diritti fondamentali. I dati che sono accessibili a tutti gli utenti di Internet senza condizioni preliminari o che possono essere visualizzati da tutti gli utenti registrati su una piattaforma (indipendentemente da un rapporto stretto con la persona che divulga le informazioni) non possono più essere classificati come "privati", indipendentemente dal contenuto. Le informazioni che sono già di dominio pubblico non sono più protette (ad eccezione del "diritto all'oblio" previsto dalla legge sulla protezione dei dati).

Se l'accesso ai dati generalmente accessibili non è una misura coercitiva, ciò 35 significa anche che l'art. 32 lett. a CDC non ha natura costitutiva ma puramente dichiarativa: se l'accesso alle fonti pubbliche non viola la sovranità dello Stato a causa della mancanza di un effettivo esercizio di coercizione, non è nemmeno necessario un accordo intergovernativo. Di conseguenza, anche i dati accessibili al pubblico provenienti da Paesi terzi che non hanno ratificato il CCC possono essere consultati senza problemi. Quest'ultimo aspetto è talvolta giustificato anche dal fatto che l'accesso transnazionale ai "dati open source" è una questione di diritto internazionale consuetudinario; tali atti di indagine sono considerati incontestabili.

Anche se questo non fosse seguito in termini così assoluti, l'intercettazione di 36 dati divulgati volontariamente - come i contenuti delle comunicazioni nei social media - non potrebbe essere considerata una violazione dei diritti fondamentali. Infatti, decidendo consapevolmente di condividere informazioni personali, le persone interessate rinunciano alla loro autodeterminazione informativa in merito a questi dati specifici, o in altre parole: rilasciandoli nel pubblico dominio, hanno appena esercitato la loro autodeterminazione informativa. Lo stesso vale per la traccia di dati pubblici lasciata dai loro stessi input, come le transazioni effettuate con Bitcoin che sono tracciabili sulla blockchain pubblica. Inoltre, i dati che non possono essere attribuiti direttamente a una persona specifica non sono degni di essere protetti da alcun titolo di diritti fondamentali. Ciò include, ad esempio, l'uso

di "Google Earth" o i dati tecnici che un server web rivela. Di conseguenza, l'acquisizione e l'analisi di informazioni personali non volontariamente divulgate è il massimo che si possa considerare una misura coercitiva; in questo caso si potrebbe legittimamente sostenere che le persone interessate non hanno alcun controllo sulle informazioni che le riguardano disponibili su Internet. Tuttavia, anche in questo caso si dovrebbe tenere conto del fatto che l'OSINT è un intervento relativamente meno invasivo e quindi proporzionato, poiché si limita a informazioni accessibili a chiunque senza particolari restrizioni di accesso.

C. Prerequisiti per l'accesso ai dati consentito dal diritto processuale penale svizzero

- 37 L'accesso ai dati "open source" è consentito per qualsiasi reato (crimine, delitto o infrazione) nella misura in cui la raccolta di prove disponibili in forma elettronica sia utile per il suo perseguimento (cfr. art. 25 cpv. 1 e art. 14 cpv. 2 lett. c CP). Nella misura in cui la legge sulla polizia cantonale lo consente, è possibile accedere alle informazioni pubbliche anche nell'ambito dell'attività di polizia preventiva.
- 38 A causa dell'assenza di violazione dei diritti fondamentali, le indagini "open source" non devono essere classificate come misure coercitive ai sensi dell'art. 196 e seguenti del CPP (cfr. sopra, n. 32 e seguenti). Di conseguenza, non sono applicabili né le disposizioni formali e sostanziali sulle perquisizioni (art. 246 e segg. CPP) né quelle sui sequestri (art. 263 CPP). Piuttosto, l'"OSINF" o "OSINT" è considerata una raccolta di prove consentita in base all'art. 95 CPP ai sensi dell'art. 139 cpv. 1 CPP.
- 39 L'accesso ai social media o alle chat room sotto falsa identità da parte di membri delle forze dell'ordine per accedere ai contenuti ivi pubblicati non deve essere classificato come una ricerca sotto copertura (art. 298a CPP) o un'indagine sotto copertura (art. 285a CPP), poiché in questo caso non si stabilisce un contatto diretto con la persona oggetto dell'indagine. La situazione sarebbe diversa se l'investigatore inviasse attivamente all'obiettivo una richiesta di amicizia o simili per prendere nota anche dei suoi contributi (privati), o se accedesse a una chat o a un forum non generalmente accessibili creando una leggenda.

Il valore probatorio dei dati disponibili al pubblico deve essere esaminato in 40
dettaglio nell'ambito della libera valutazione delle prove (art. 10 cpv. 2 CPP). A
questo proposito, sono diverse le considerazioni da fare, in primo luogo
l'origine della prova, la sua autenticità e affidabilità, il rapporto del suo autore
con le parti del procedimento, ma soprattutto il fatto che la fonte sia anonima
o nota, soprattutto perché i dubbi sono grandi in caso di origine sconosciuta e
i dati sono relativamente facili da manipolare. È inoltre importante che i dati
siano protetti dal punto di vista forense secondo l'attuale stato dell'arte,
poiché i metadati possono essere utilizzati per trarre conclusioni sul valore
delle prove; a tal fine non è sufficiente prendere semplicemente degli
screenshot.

III. ACCESSO AD ALTRI DATI CONSERVATI IN UN ALTRO STATO CONTRAENTE (LETT. B)

A. Consenso legittimo e volontario della persona legittimamente autorizzata a divulgare i dati

1. Diritto alla divulgazione

L'art. 32 del CDC regola solo l'ammissibilità dell'accesso ai dati ai sensi del 41
diritto internazionale; "le norme nazionali in base alle quali deve essere
valutato il trasferimento dei dati, ossia in base alle quali si deve decidere se il
consenso al trasferimento è stato legittimamente dato da una persona
legittimamente autorizzata a farlo, non sono influenzate dalla Convenzione". Il
Consiglio d'Europa si è astenuto dal definire il concetto di autorizzazione al
trasferimento in modo più dettagliato nella Convenzione. La relazione
esplicativa afferma che chi può dare il consenso "può variare a seconda delle
circostanze, della natura della persona e della legge applicabile".

La questione di chi sia "legalmente autorizzato a divulgare i dati [...]" è 42
determinata dal diritto interno dello Stato richiedente, ossia quello in cui si
svolge l'indagine. Ciò sembra ragionevole anche perché spesso non è
possibile, o non senza grandi sforzi, localizzare con precisione i dati prima di
accedervi. Sarebbe inoltre impraticabile e incompatibile con l'idea di
accelerazione del CCC richiedere alle autorità svizzere di verificare
separatamente la situazione delle autorizzazioni per ogni Stato contraente
prima di poter effettuare il backup dei dati.

- 43 L'autorizzazione a trasmettere i dati è necessaria. Necessario, ma anche sufficiente, è il consenso di una persona legittimamente autorizzata a comunicarli alle autorità di contrasto. L'autorizzazione può essere di natura legale o obbligatoria.
- 44 Contrariamente al messaggio, non è un requisito aggiuntivo che il consenso debba essere dato da "una persona nel paese"; l'art. 32 lett. b CPC non conosce un criterio così restrittivo, che peraltro sarebbe in contrasto con lo spirito e lo scopo della Convenzione.
- 45 Il Rapporto esplicativo e il Dispaccio citano come soggetti legittimati al consenso le persone che hanno la propria posta elettronica archiviata presso un fornitore di servizi in un altro Paese o altri dati archiviati all'estero. Nella letteratura, il cliente che affitta lo spazio di archiviazione è indicato come persona autorizzata nel caso di dati archiviati su server cloud, la banca nel caso di dati su transazioni finanziarie, il datore di lavoro per l'account di posta elettronica aziendale e, nel caso di persone giuridiche, le persone dichiarate responsabili internamente, in mancanza di tali regolamenti interni, il consiglio di amministrazione (AG) o la direzione (GmbH); è probabile che gli amministratori o altre persone autorizzate all'accesso manchino di tale autorizzazione su base regolare.
- 46 Un aspetto che non è stato discusso in modo conclusivo nella relazione esplicativa riguarda la questione se il consenso debba sempre essere dato dagli interessati (responsabili del trattamento) o se sia sufficiente l'autorizzazione di altri organismi che trattano i dati personali (in primo luogo il fornitore di servizi Internet come responsabile del trattamento). L'estensione ai fornitori di servizi Internet è vista in modo critico, perché essi si limiterebbero a esercitare la custodia dei dati e non sarebbero quindi in grado di dare un consenso legalmente valido.
- 47 La questione del diritto di trasmettere i dati deve essere considerata nel contesto più ampio in cui, secondo la situazione giuridica attuale in Svizzera, non esiste un diritto di proprietà sui dati: Il diritto di proprietà ai sensi dell'art. 641 del CC si estende solo alla "cosa", che la dottrina intende come "un oggetto fisico, distinto dagli altri, che sia accessibile a un controllo effettivo e legale". Poiché i dati sono beni immateriali, non è possibile stabilire una proprietà ai sensi dell'art. 641 CC su di essi (ma certamente non sui sistemi di elaborazione dati o sui supporti di dati). Inoltre, la legge sul diritto d'autore

copre solo le creazioni intellettuali a carattere individuale in forma di dati ed è applicabile solo in casi eccezionali. Tuttavia, il diritto di accesso ai dati è riconosciuto dalla legge sulla protezione dei dati, almeno per quanto riguarda i dati personali, per i quali il diritto di accesso è normato dall'art. 25 della Legge federale sulla protezione dei dati del 25.9.2020 ("LPD", RS 235.1). L'art. 28 LPD garantisce inoltre agli interessati il diritto alla cessione e al trasferimento dei dati personali (portabilità dei dati) se sono soddisfatte determinate condizioni, a condizione che abbiano comunicato tali dati ai responsabili del trattamento. Inoltre, i dati personali "possono essere ottenuti solo per uno scopo specifico e riconoscibile dall'interessato; possono essere trattati solo in modo compatibile con tale scopo" (art. 6 cpv. 3 LPD). La consegna dei dati personali alle autorità di polizia è una forma di trattamento dei dati (cfr. art. 5 lett. d LPD). In altre parole: La persona autorizzata può acconsentire alla divulgazione da parte del responsabile del trattamento.

La Svizzera, in linea con altri Stati contraenti, consente quindi che il consenso dei fornitori di servizi Internet sia sufficiente come conseguenza del loro rapporto di diritto privato con la persona interessata, se i fornitori di servizi hanno previsto un diritto di trasmissione alle autorità di contrasto straniere nelle loro condizioni generali di utilizzo o nelle linee guida sull'utilizzo dei dati. La maggior parte dei fornitori di servizi Internet prevede nei propri contratti d'uso che i dati possano essere divulgati non solo in presenza di un'ordinanza giudiziaria valida, ma anche su semplice richiesta delle autorità di polizia o che i fornitori collaborino con le autorità di polizia. In questi casi, la divulgazione è conforme alla legge. 48

2. Consenso

Il fatto che una società estera interessata abbia in linea di principio il diritto di dichiarare il proprio consenso alla divulgazione diretta dei dati nel senso descritto non è sufficiente (secondo la chiara formulazione dell'art. 32 lett. b del Codice civile) per l'accesso transfrontaliero: Occorre piuttosto verificare se l'autorità di contrasto richiedente ha ottenuto un "consenso legittimo e volontario" giuridicamente efficace. 49

Allo stato attuale, una persona giuridica o una persona fisica capace di intendere e di volere, che sia autorizzata a disporre dei dati sulla base di un'autorizzazione legale o obbligatoria e a consentire a terzi di accedervi, è in grado di dare il proprio consenso (cfr. anche sopra, n. 43 e segg.). Se vi sono 50

più persone autorizzate a divulgare i dati, è sufficiente il consenso di una sola persona. Se, ad esempio, il titolare del conto ha dato la sua autorizzazione, non è necessario un ulteriore consenso da parte della società estera fornitrice. Al contrario, è sufficiente che il provider straniero, sulla base di una corrispondente autorizzazione del cliente nelle condizioni generali di utilizzo, rilasci i dati (per il consenso da parte dei fornitori di servizi Internet, si veda sopra, n. 46 e seguenti).

- 51 Secondo i principi generali di procedura penale, il consenso può essere dichiarato espressamente (per il quale non esiste un requisito formale) o implicito. Quest'ultimo caso si verifica se la persona richiesta dalle autorità di contrasto - ad esempio un fornitore di servizi o il proprietario dell'account in questione - fornisce i dati su richiesta.
- 52 Allo stesso tempo, ciò significa che le corrispondenti "richieste di informazioni" possono essere fatte all'estero senza che ciò si qualifichi come un atto inammissibile in uno Stato estero. In pratica, le richieste dirette ai provider stranieri sono diventate uno standard internazionale, che può essere inserito attraverso i portali di applicazione della legge gestiti dai provider stessi o, nel caso di altri provider (più piccoli), può essere consegnato anche attraverso la polizia (tramite Interpol). Diversi trattati internazionali consentono la notifica diretta di documenti ufficiali all'estero, almeno in linea di principio, primo fra tutti l'art. 52 cpv. 1 della Convenzione di Schengen del 19 giugno 1990 ("CISA"). Tuttavia, questa Convenzione prevede che ogni Stato possa o debba dichiarare quali documenti possono essere inviati a persone sul suo territorio. Di conseguenza, occorre verificare separatamente per ogni Stato contraente se la notificazione diretta è consentita e, in caso affermativo, in quale misura. Nella misura in cui i destinatari vengono informati che la collaborazione è volontaria e che un eventuale rifiuto non comporta conseguenze negative dirette, non è chiaro in che misura ciò possa essere considerato una violazione della sovranità territoriale straniera e quindi un caso di applicazione dell'art. 52 cpv. 1 della Convenzione di Schengen - si tratta di semplici inviti senza alcuna minaccia di coercizione e senza conseguenze negative legate a un eventuale rifiuto di collaborare. Non avrebbe quindi molto senso se l'eccezione di cui all'art. 32 lett. b CDC fosse intesa ad aumentare l'efficienza della macchinosa procedura formale di assistenza reciproca, ma allo stesso tempo venisse silurata dall'obbligo di chiarire la volontà delle persone interessate di cooperare volontariamente

attraverso questa stessa procedura formale di assistenza reciproca. A questo proposito, l'art. 32 lett. b CPC prevale sull'art. 52 CAAS.

Il consenso deve essere volontario; la persona interessata non deve essere 53
ingannata o costretta a consegnare i dati. Spesso vi è una pressione indiretta, in quanto l'ufficio del pubblico ministero può richiedere il sequestro e il trasferimento dei dati in questione attraverso l'assistenza giudiziaria se la persona si rifiuta. Tuttavia, ciò non è sufficiente a compromettere la formazione della volontà. Lo stesso vale, ad esempio, nel caso di una situazione di detenzione, in cui l'imputato potrebbe sentirsi soggettivamente costretto a collaborare a causa delle circostanze e a fornire i dati conservati all'estero per essere rilasciato dalla detenzione il più rapidamente possibile. Tuttavia, anche una situazione di pressione generale di questo tipo non impedisce all'imputato di dare il proprio consenso in conformità alla legge. Ciò che è vietato, invece, è la minaccia concreta di possibili ulteriori svantaggi. Di conseguenza, una persona domiciliata in Svizzera non può essere costretta a produrre i dati archiviati all'estero a cui ha accesso. Tuttavia, può essere invitata a farlo mediante un ordine di divulgazione (art. 265 CPP).

Infine, il consenso può essere revocato in qualsiasi momento, ma la revoca è 54
valida solo ex nunc. Una revoca successiva al salvataggio dei dati è pertanto irrilevante.

B. Conseguenze di un consenso legalmente valido

Se la persona autorizzata a disporre divulga volontariamente i propri dati di 55
accesso a servizi Internet di derivazione straniera o acconsente alla ricerca online, le autorità preposte all'applicazione della legge, in applicazione dell'art. 32 lett. b CPC, possono accedere direttamente alle informazioni e metterle al sicuro utilizzando i dati di accesso. Inoltre, ogni persona privata è libera di mettere a disposizione delle autorità di polizia copie dei propri dati archiviati presso un provider estero (come e-mail o messaggi di chat). È anche possibile che l'autorità giudiziaria chieda direttamente a un fornitore di servizi Internet domiciliato all'estero di consegnare i dati (cfr. sopra, n. 48, 51 s.).

C. Presupposti per l'accesso ai dati consentito dal diritto processuale penale svizzero

- 56 L'accesso a dati non pubblici in Svizzera non è possibile senza condizioni preliminari. Nel caso dei dati relativi al contenuto, i dati devono essere sequestrati (ad esempio tramite un ordine di edizione [art. 265 CPP] o durante una perquisizione domiciliare [art. 244 CPP]), perquisiti (art. 246 CPP) e quindi, se rilevanti ai fini della prova, sequestrati (art. 263 CPP). Per i dati sul traffico, una raccolta marginale retroattiva di dati (Art. 273 CPP) deve essere ordinata e approvata dal tribunale dei provvedimenti coercitivi (Art. 274 CPP). L'art. 32 lett. b CPC non costituisce una misura indipendente per la conservazione o la raccolta di prove che superi i requisiti nazionali. La disposizione prevede solo che, in presenza di un consenso legalmente valido, si possa rinunciare a una procedura di assistenza giudiziaria. L'accesso ai dati, anche se avviene a livello transnazionale, costituisce quindi una misura coercitiva nazionale che deve soddisfare le leggi nazionali. Il sequestro di dati all'estero deve quindi soddisfare - oltre al consenso descritto - le stesse condizioni che si avrebbero se i dati fossero conservati in Svizzera. Una "richiesta di informazioni" a un fornitore di servizi Internet deve quindi essere qualificata come un ordine di divulgazione ai sensi dell'art. 265 CPP.
- 57 In primo luogo, ne consegue che, in linea di principio, l'apertura di un'indagine penale ai sensi dell'art. 309 cpv. 1 CPP e quindi un sufficiente sospetto di reato sono un prerequisito, per cui un procedimento penale non ancora formalmente aperto si considera automaticamente aperto con l'intercettazione dei dati (art. 309 cpv. 1 lett. b CPP). Nei procedimenti d'indagine di polizia indipendenti, l'art. 32 lett. b CPC non può essere invocato. Anche i servizi di intelligence non possono invocarlo.
- 58 Il CCC serve a raccogliere le prove di un reato che sono disponibili in forma elettronica (cfr. art. 25 cpv. 1 e art. 14 cpv. 2 lett. c CCC). Il sospetto sufficiente può quindi estendersi in linea di principio a qualsiasi reato, purché vi sia almeno il sospetto criminologico che sia stato commesso con un dispositivo tecnico. La gravità del reato è irrilevante: l'accesso transnazionale ai dati è in linea di principio aperto ai reati, alle infrazioni e alle trasgressioni (nei casi minori, tuttavia, la proporzionalità dell'accesso ai dati può essere oggetto di discussione).

Per il sequestro dei dati sui contenuti, è necessario presupporre che essi 59
 contengano informazioni soggette a sequestro (art. 246 CPP). Ai sensi dell'art.
 263 cpv. 1 lett. a CPP, gli oggetti appartenenti a un imputato o a terzi possono
 essere sequestrati in particolare se sono necessari come prova. Per il
 sequestro e la perquisizione di registri, è sufficiente una potenziale rilevanza
 come prova, che è data se i dati "possono essere importanti per il chiarimento
 dei presunti reati" o non appaiono "palesamente inidonei". La giurisprudenza
 non stabilisce standard elevati in merito. Infine, il sequestro e la perquisizione
 devono essere proporzionati (art. 197 cpv. 1 lett. c e d CPP) e quindi adeguati,
 necessari e appropriati. Soprattutto nel perseguimento dei reati, la
 proporzionalità può essere discutibile. Da un punto di vista formale, il
 sequestro e la perquisizione da parte del pubblico ministero devono di norma
 essere ordinati in un mandato scritto (art. 241 cpv. 1 CPP). Per la raccolta dei
 dati di inventario, invece, l'unico requisito è che vi sia il sospetto che sia stato
 commesso un reato tramite Internet (art. 22 cpv. 1 della Legge federale
 sull'intercettazione del traffico postale e delle telecomunicazioni del 18.3.2016
 ["BÜPF"; RS 780.1]).

Se i dati della cronologia/log IP o altri dati marginali sono raccolti all'estero, si 60
 pone la questione se l'ufficio del pubblico ministero possa rendere disponibili
 tali registrazioni di propria competenza o se debba essere ottenuta
 l'autorizzazione dal tribunale per i provvedimenti coercitivi in applicazione
 dell'art. 273 cpv. 2 CPP. Il Tribunale federale ha stabilito che l'art. 273 CPP
 consente la raccolta retroattiva di dati marginali sul traffico delle
 telecomunicazioni solo "presso i fornitori di servizi di telecomunicazione o di
 accesso a Internet domiciliati in Svizzera e soggetti al diritto svizzero". Ha
 quindi escluso la sua applicabilità a situazioni internazionali, con la
 conseguenza che per la raccolta non dovrebbe essere necessaria
 l'autorizzazione del tribunale dei provvedimenti coercitivi; in altre parole,
 l'art. 32 lett. b CPC consente "uno scambio internazionale facilitato di dati
 marginali". In un'altra decisione, tuttavia, il Tribunale federale ha respinto una
 richiesta di autorizzazione da parte dell'ufficio del pubblico ministero sulla
 base del fatto che i requisiti dell'art. 32 lett. b CPC non erano stati soddisfatti
 in questo caso, aggiungendo che l'accesso diretto transfrontaliero avrebbe
 dovuto essere autorizzato dal tribunale per i provvedimenti obbligatori ai
 sensi dell'art. 273 CPP. Inoltre, in un'ulteriore sentenza, ha espressamente
 affermato che l'autorizzazione del tribunale dei provvedimenti coercitivi deve
 essere ottenuta anche per le cronologie IP interrogate da provider stranieri e

che, poiché ciò non è stato fatto nel caso specifico, le conoscenze ottenute dalle interrogazioni erano assolutamente inutilizzabili. Il fatto che il Tribunale federale si sia occupato dell'art. 273 CPP può sembrare comprensibile a prima vista se si considera la natura giuridica dell'art. 32 lett. b del CPP, che si limita a dichiarare ammissibile l'accesso transnazionale in base al diritto internazionale, ma non incide sulle disposizioni nazionali, in particolare per quanto riguarda la competenza a raccogliere dati. Occorre tuttavia considerare che le disposizioni sulla raccolta retroattiva di dati marginali non sono attivate unicamente dal tipo di dati da raccogliere (traffico o dati marginali), ma i dati devono essere ottenuti da un fornitore di telecomunicazioni o essere protetti dal segreto delle telecomunicazioni (art. 321^{ter} CP e art. 43 della legge sulle telecomunicazioni del 30.4.1997 ["TCA"; RS 784.10]). Tuttavia, il segreto sulle telecomunicazioni si applica (nella misura in cui è di interesse in questo caso) solo ai fornitori che offrono accesso a Internet o trasmissione di telecomunicazioni. I fornitori di servizi Internet o di servizi di comunicazione derivati che non offrono accesso a Internet ma solo servizi forniti via Internet ("servizi over-the-top") non sono considerati fornitori di telecomunicazioni. Per questo motivo, né il sequestro di dati marginali di tali società in patria né all'estero è soggetto a un obbligo di licenza. A tal fine è sufficiente un ordine di modifica all'attenzione del fornitore di servizi Internet (art. 265 CPP). Di conseguenza, se le cronologie IP e altri dati marginali vengono raccolti da fornitori di servizi non di telecomunicazione all'estero sulla base dell'art. 32 lett. b CPC, non è necessario ottenere un'autorizzazione dal tribunale per i provvedimenti coercitivi.

- 61 Infine, ci si chiede in che misura gli altri requisiti per l'assistenza giudiziaria, ossia i motivi di rifiuto e la necessità della doppia incriminazione, si applichino anche all'art. 32 lett. b CPC. L'art. 25 par. 4 CPC prevede, al titolo 3 ("Principi generali dell'assistenza giudiziaria"), che, a meno che il CPC non disponga espressamente altrimenti, "l'assistenza giudiziaria è soggetta alle condizioni previste dalla legge della Parte richiesta o dai trattati di assistenza giudiziaria applicabili, compresi i motivi per cui la Parte richiesta può rifiutare di cooperare". Tuttavia, l'art. 32 lett. b CPC consente l'accesso diretto prima dell'assistenza reciproca; in questo caso non è necessaria una "richiesta" all'altro Stato contraente, come invece prevede l'art. 25 cpv. 4 CPC. Di conseguenza, l'accesso concesso volontariamente non richiede la doppia incriminazione, né devono essere soddisfatte ulteriori condizioni che

altrimenti si applicherebbero ai procedimenti di assistenza giudiziaria. Questo ammorbidimento è giustificato, da un lato, dalla natura volontaria dei consenzienti e, dall'altro, dalla natura giuridica dell'art. 32 lett. b CPC, che estende il braccio territoriale delle autorità giudiziarie, pur continuando a essere una misura nazionale di conservazione delle prove. Se il tentativo di sequestrare le registrazioni sulla base dell'art. 32 lett. b CPC fallisce, si deve percorrere la via dell'assistenza giudiziaria ordinaria, per la quale si applicano nuovamente le relative limitazioni.

L'interessato non può difendersi dal sequestro diretto in quanto tale o ⁶² dall'indagine del provider; tuttavia, il rimedio legale del sigillo (art. 248 CPP) è a sua disposizione contro la perquisizione, nella misura in cui può dimostrare in modo credibile un divieto di sequestro (art. 264 CPP). L'effetto dell'apposizione del sigillo è che le autorità giudiziarie non possono consultare i documenti fino a quando il tribunale per i provvedimenti coercitivi non si sia pronunciato sull'ammissibilità della raccolta e della ricerca dei dati.

IV. CONSERVAZIONE DELLE PROVE AL DI LÀ DELL'ART. 32 CPC SECONDO IL PRINCIPIO DELL'ACCESSO

In attrito con il principio di territorialità, che si basa sul luogo di ⁶³ conservazione delle prove e quindi, nel caso dei dati, sul luogo fisico di conservazione, il Tribunale federale consente l'accesso anche in assenza di consenso, indipendentemente dal luogo in cui i dati sono conservati al momento dell'accesso; il fattore decisivo è che i dati siano accessibili dalla Svizzera: "Chiunque utilizzi un servizio Internet derivato offerto da una società estera tramite un accesso Internet in Svizzera non agisce all'estero. Anche il semplice fatto che i dati elettronici del relativo servizio Internet derivato siano gestiti su server (o supporti di memorizzazione cloud) all'estero non fa sì che una ricerca online condotta dalla Svizzera in conformità alla legge appaia come un atto investigativo inammissibile in territorio straniero (ai sensi della prassi esposta) [...]".

L'oggetto della valutazione era l'accesso all'account Facebook di una persona ⁶⁴ accusata di traffico qualificato di stupefacenti, i cui dati di accesso erano stati messi a disposizione dalle autorità giudiziarie. L'ufficio del pubblico ministero ha quindi fatto cercare l'account Facebook utilizzando i dati di accesso

identificati e ha sequestrato i messaggi di chat rilevanti per le prove. All'epoca il luogo di archiviazione di questi dati non si trovava - e non si trova tuttora - in Svizzera. Nella sentenza citata, il Tribunale federale ha stabilito che gli account di imputati o di terzi su servizi Internet stranieri possono essere consultati direttamente se sono soddisfatti i requisiti generali di una perquisizione ai sensi del CPP e se gli investigatori agiscono "da computer, server e infrastrutture informatiche situati in Svizzera", ossia se rimangono fisicamente in Svizzera.

- 65 La prassi ha accolto con favore questa giurisprudenza. È applicabile non solo a Facebook, ma a un'ampia gamma di servizi nazionali ed esteri, quali host provider, servizi di comunicazione, servizi cloud, fornitori di outsourcing di dati, forum di chat, piattaforme di scambio di documenti, portali di shopping e fornitori di servizi di posta elettronica. Anche i beni in criptovaluta detenuti in un hot wallet possono essere sequestrati (cioè solitamente trasferiti a un wallet delle forze dell'ordine) in applicazione di questa giurisprudenza. Anche la giurisprudenza del tribunale federale sta diventando sempre più importante. La tendenza generale per i dispositivi elettronici è quella di abbandonare l'archiviazione individuale e di metterli al sicuro nel cloud. I telefoni cellulari, in particolare, vengono spesso utilizzati dagli utenti solo come "chiavi" per vari servizi, per cui i dati in questione non vengono più memorizzati sul dispositivo fisico. Se un telefono cellulare o un tablet viene sequestrato durante una perquisizione domiciliare o un fermo di polizia e si scopre che i dati non sono memorizzati sul dispositivo ma nel cloud, o se sul dispositivo vengono trovate applicazioni di servizi di comunicazione o provider di e-mail web, tutti questi dati possono essere sequestrati in base alla giurisprudenza della Corte Suprema Federale. In pratica, questa procedura è facilitata dal fatto che gli utenti spesso salvano i propri dati di accesso ai servizi Internet nel gestore di password o in un browser Internet per motivi di comodità o utilizzano la stessa password per diversi servizi. Inoltre, durante le perquisizioni domiciliari presso le aziende, si scopre sempre più spesso che queste non ospitano o archiviano più i propri dati presso la sede centrale o il luogo di gestione, ma hanno esternalizzato l'elaborazione e l'archiviazione dei dati a fornitori di servizi esterni. In queste situazioni, anche la decisione del Tribunale federale citata è utile, in quanto consente il backup dei dati anche in questi casi.

Nella decisione citata, il Tribunale federale ha implicitamente invocato il cosiddetto "principio di accesso". In base a questo principio, nel caso dei dati informatici, non si fa affidamento sull'ubicazione del supporto su cui sono memorizzate le informazioni, ma piuttosto su chi ha accesso ai dati rilevanti per il procedimento e da dove. Il controllo sui dati spetta alla persona che ha l'autorizzazione all'accesso e non alla persona che è in possesso fisico del supporto dati. Alcuni autori citano questo aspetto come una ragione per cui la ricerca e il sequestro di dati archiviati all'estero da parte delle autorità svizzere in Svizzera non dovrebbero essere considerati una violazione della sovranità. In altre parole, l'ammissibilità dell'accesso online dovrebbe dipendere esclusivamente dalla legalità dell'atto investigativo nazionale. 66

Tuttavia, l'accesso a fonti estere non accessibili al pubblico, in particolare quelle protette da password o altre barriere, ha un forte impatto sul territorio estero ("digitale"). Per questo motivo, l'accesso delle autorità investigative ai dati all'estero è talvolta visto come una violazione della sovranità dello Stato in questione; tali prove possono essere ottenute solo attraverso l'assistenza giudiziaria internazionale o direttamente se ciò è esplicitamente previsto da accordi internazionali. In realtà, il principio dell'accesso non cambia gli effetti dell'accesso online dello Stato sulla sovranità straniera, dove si verifica l'effettivo successo della misura. Certo, l'assenza di azioni fisiche da parte di funzionari sul territorio straniero non dovrebbe ancora superare i limiti tracciati dall'art. 299 CP. Tuttavia, per quanto riguarda l'intensità del loro intervento, essi non sono affatto inferiori ad attività investigative fisiche equivalenti (la ricerca del supporto di memorizzazione all'estero da parte di funzionari svizzeri), che sarebbero chiaramente inammissibili. Inoltre, il reperimento online dà il via a operazioni di elaborazione dei dati all'estero; l'accesso lascia tracce rintracciabili nello Stato di destinazione. Nel peggiore dei casi, l'agente investigativo può essere perseguito per intrusione non autorizzata in un sistema di elaborazione dati, acquisizione non autorizzata di dati o inosservanza di diritti sovrani stranieri, a seconda della legislazione nazionale. Inoltre, la raccolta di prove digitali dalla Svizzera avviene in segreto per lo Stato estero, il che - visti gli scandali dei servizi segreti del recente passato - la rende ancora più pericolosa dal suo punto di vista. È sorprendente che, secondo uno studio dell'ONU, il diritto nazionale di diversi Stati consenta comunque una sorta di accesso diretto ai dati archiviati all'estero, mentre la percentuale di Stati che consente tale accesso diretto da parte delle forze dell'ordine straniere è notevolmente inferiore, secondo lo stesso studio. Il 67

senso del diritto internazionale sembra quindi essere maggiore quando viene colpita la propria sovranità rispetto a quando si dipende dall'ottenimento di prove all'estero. In ogni caso, la Convenzione sulla criminalità informatica consente già l'accesso diretto ai dati stranieri in modo limitato all'art. 32 CCC; un ulteriore reperimento di prove - almeno nei rapporti tra gli Stati della Convenzione - deve essere visto al contrario come un'invasione della sovranità statale. Non a caso il Consiglio d'Europa ha previsto espressamente l'art. 31 CPC, intitolato "Assistenza reciproca nell'accesso ai dati memorizzati". Una proposta avanzata dagli Stati membri dell'UE nel contesto dei negoziati, secondo la quale le ricerche online transnazionali dovrebbero essere consentite in casi urgenti, non è stata accolta - a causa della mancanza di consenso, si è deciso di non regolamentare tali situazioni. Anche gli sforzi ripresi da allora sono rimasti in gran parte infruttuosi; anche il 2° Protocollo aggiuntivo al TCC non è un grande successo in questo senso. L'accesso diretto transnazionale ai dati senza il consenso di una persona autorizzata non è quindi ancora oggetto di un consenso internazionale, viola la sovranità dello Stato interessato ed è quindi contrario al diritto internazionale fino a quando non ci saranno ulteriori sviluppi degli attuali accordi bilaterali o multilaterali.

- 68 Questo risultato è insoddisfacente. In primo luogo, soprattutto quando c'è il rischio che i dati vadano persi senza un'azione immediata. È quindi concepibile consentire il congelamento transnazionale provvisorio dei dati in costellazioni eccezionali in cui vi è un rischio di collusione o di perdita di prove, se anche una "richiesta di conservazione" ai sensi dell'art. 29 del Codice penale sarebbe presentata troppo tardi. In questo caso, i dati conservati dovrebbero essere conservati separatamente e non potrebbero essere consultati fino alla successiva richiesta di autorizzazione allo Stato contraente interessato. In secondo luogo, la critica di cui sopra si basa sul presupposto che le autorità di contrasto siano a conoscenza, al momento dell'accesso, del fatto che i dati non sono conservati nel loro Paese. Tuttavia, spesso non è chiaro fin dall'inizio dove siano conservati i dati, se localmente sul dispositivo o nel cloud. Anche in questi casi deve essere consentito conservare le prove, se necessario con una successiva richiesta di assistenza reciproca nel caso in cui si scopra che i dati sono archiviati all'estero (cfr. sopra, n. 23).

V. CONSEGUENZE DELLA VIOLAZIONE DEL DIRITTO DI SOVRANITÀ STRANIERA

Se i poteri del CCC vengono oltrepassati, l'assistenza giudiziaria in materia penale viene aggirata attraverso l'accesso diretto a vettori di dati stranieri e viene così violato il principio di territorialità o di sovranità, si pone la questione dell'inutilizzabilità delle prove così ottenute. In linea di principio, l'elusione del canale di assistenza giudiziaria può essere contestata nei procedimenti penali nazionali. 69

I tribunali cantonali si sono finora pronunciati a favore di un divieto relativo di sfruttamento ai sensi dell'art. 141 cpv. 2 CPP, in base al quale la prova in questione può essere sfruttata nella misura in cui è necessaria per chiarire un reato grave. È tuttavia discutibile se il principio di territorialità del diritto internazionale e l'obbligo di ricorrere alla via dell'assistenza giudiziaria siano in realtà solo disposizioni valide o se, in considerazione della loro importanza, si debba presumere un divieto assoluto di utilizzo delle prove (ad esempio sotto forma di violazione dell'ordine pubblico). Il Tribunale federale ha deciso in questa direzione quando ha ritenuto assolutamente inutilizzabile una misura di sorveglianza segreta (localizzatore GPS e dispositivi di ascolto in un veicolo utilizzato anche per viaggi all'estero) per quanto riguarda i viaggi all'estero. Tuttavia, sembra possibile e ragionevole adottare l'opinione sostenuta in Germania, secondo la quale la questione dell'utilizzabilità dipende dal fatto che l'investigatore fosse consapevole, al momento della raccolta dei dati, che l'accesso non sarebbe stato conforme al diritto internazionale. Se non ne era a conoscenza, deve essere possibile far eseguire una successiva procedura formale di assistenza reciproca (nel senso di una procedura di autorizzazione) per le prove (oggettivamente ottenute in modo illegale) al fine di evitare l'inutilizzabilità delle prove. 70

Quest'ultimo punto è particolarmente applicabile ai casi in cui non è chiaro fin dall'inizio dove siano conservati i dati: Se non è possibile escludere un luogo di conservazione all'interno del Paese, l'accesso per preservare le prove deve essere consentito; la conoscenza positiva del luogo di conservazione non è un prerequisito. "La mera possibilità di un luogo di archiviazione all'estero non può far scattare l'obbligo di assistenza reciproca, soprattutto perché in questi casi non è possibile determinare quale paese sarà effettivamente interessato". Se successivamente dovesse risultare (ad esempio anche a seguito 71

di corrispondenti reclami da parte della difesa) che i dati intercettati non sono stati memorizzati in Germania e nemmeno in uno Stato contraente, sarà necessario ottenere una successiva autorizzazione nello Stato interessato tramite l'assistenza reciproca.

VI. NECESSITÀ DI UNA RIFORMA

- 72 Il Consiglio d'Europa ha riconosciuto la necessità di ammorbidire tempestivamente i principi territoriali a causa degli sviluppi tecnologici e ha emanato una disposizione progressiva nell'art. 32 CCC rispetto alle tradizionali convenzioni di assistenza giudiziaria. Idee più avanzate erano altrettanto visionarie, poiché non erano (ancora) in grado di ottenere il sostegno della maggioranza a causa dell'idea fortemente ancorata di sovranità. Tuttavia, se la comunità degli Stati vuole un'applicazione della legge efficace e in grado di svolgere i propri compiti anche nel XXI secolo, sembra necessario e sensato rinunciare completamente alla sovranità in materia di dati in rete. Oggi non si tratta più solo di criminalità transfrontaliera, che è sempre stata difficile da comprendere per le forze dell'ordine nazionali, ma anche i casi puramente nazionali non possono più essere risolti in breve tempo a causa dello spostamento delle prove oltre i confini nazionali, e tanto meno con un adeguato rapporto costi-benefici.
- 73 Certo, per il momento sembra più promettente preparare dei panetti più piccoli: in primo luogo, la Svizzera dovrebbe firmare e ratificare al più presto il 2° Protocollo aggiuntivo al CCC, anche se non si tratta di quello più grande. In secondo luogo, molto sarebbe già fatto se, nel contesto dell'art. 32 lett. b CDC, ci si mettesse al passo con la realtà giuridica e non ci si limitasse più a collegare il luogo di conservazione, ma piuttosto (anche) al domicilio della persona avente diritto all'accesso o al fatto che un'azienda offra i propri servizi nello Stato in questione (cfr. sopra, n. 25). In terzo luogo, la Svizzera dovrebbe cercare di associarsi al sistema e-Evidence dell'UE (anche se ciò sarà politicamente difficile da attuare). In quarto luogo, le ricorrenti discussioni sull'accesso unilaterale ai dati all'estero dovrebbero essere riprese e portate a termine. Come minimo, in futuro si dovrebbe considerare sufficiente un luogo di accesso nazionale per non dover più classificare l'accesso ai dati come una violazione della sovranità dello Stato nel luogo di conservazione. In questo contesto, per aumentare l'accettazione di tale soluzione si potrebbero includere misure e garanzie di protezione (ad

esempio, l'obbligo di informare lo Stato interessato dell'accesso, la necessità di un'autorizzazione successiva, i requisiti per lo Stato di diritto e la protezione dei diritti fondamentali, ecc.

BIBLIOGRAFIA

Abo Youssef Omar, Smartphone-User zwischen unbegrenzten Möglichkeiten und Überwachung, ZStrR 130 (2012), S. 92 ff.

Aegli Michael, Die strafprozessuale Sicherstellung von elektronisch gespeicherten Daten, Unter besonderer Berücksichtigung der Beweismittelbeschlagnahme am Beispiel des Kantons Zürich, Zürich 2004.

Bangerter Simon, Hausdurchsuchungen und Beschlagnahmen im Wettbewerbsrecht unter vergleichender Berücksichtigung der StPO, Zürich 2014.

Bär Wolfgang, Transnationaler Zugriff auf Computerdaten, ZIS 2 (2011), S. 53 ff., abrufbar unter https://www.zis-online.com/dat/artikel/2011_2_525.pdf, besucht am 17.10.2023.

Biaggini Elena, Strafrechtlicher Schutz des E-Mail-Verkehrs post mortem?, sui generis 2021, S. 321 ff., abrufbar unter <https://doi.org/10.21257/sg.196>, besucht am 17.10.2023.

Bonnici Jeanne Pia Mifsud et al., The European Legal Framework on Electronic Evidence: Complex and in Need of Reform, in: Biasiotti Maria Angela/Bonnici Jeanne Pia Mifsud/Cannataci Joe/Turchi Fabrizio (Hrsg.), Handling and Exchanging Electronic Evidence Across Europe, 2018, S. 189 ff., abrufbar unter https://link.springer.com/chapter/10.1007/978-3-319-74872-6_11, besucht am 17.10.2023.

Bottinelli Nicolas, L'obtention par l'autorité pénale des données informatiques situées à l'étranger, AJP 2016, S. 1327 ff.

Brodowski Dominik, Der «Grundsatz der Verfügbarkeit» von Daten zwischen Staat und Unternehmen, ZIS 8-9/2012, S. 474 ff., abrufbar unter https://zis-online.com/dat/artikel/2012_8-9_703.pdf, besucht am 17.10.2023.

Brodowski Dominik/Eisenmenger Florian, Zugriff auf Cloud-Speicher und Internetdienste durch Ermittlungsbehörden, Sachliche und zeitliche

Reichweite der «kleinen Online-Durchsuchung» nach § 110 Abs. 3 StPO, ZD 2014, S. 119 ff.

Burgermeister Daniel, Beweiserhebung in der Cloud, Luzern 2015, abrufbar unter https://www.unilu.ch/fileadmin/fakultaeten/rf/institute/staak/MAS_Forensics/dok/Masterarbeiten_MAS_5/Burgermeister_Daniel.pdf, besucht am 17.10.2023.

Capus Nadja, Strafrecht und Souveränität: Das Erfordernis der beidseitigen Strafbarkeit in der internationalen Rechtshilfe in Strafsachen, Basel 2010.

Cartner Anna/Schweingruber Sandra, Strafbehörden dürfen googeln, AJP 2021, S. 990 ff.

De Busser Els, Open Source Data and Criminal Investigations: Anything You Publish Can and Will Be Used Against You, Groningen Journal of International Law 2/2 (2014): Privacy in International Law, S. 90 ff., abrufbar unter https://www.researchgate.net/publication/328962642_Open_Source_Data_and_Criminal_Investigations_Anything_You_Publish_Can_and_Will_Be_Used_Against_You, besucht am 17.10.2023.

Dombrowski Nadine, Extraterritoriale Strafrechtsanwendung im Internet, Potsdam 2011/2012.

Donatsch Andreas/Lieber Viktor/Summers Sarah/Wohlens Wolfgang (Hrsg.), Schulthess Kommentar zur Schweizerischen Strafprozessordnung, 3. Aufl., Zürich 2020 (zit. SK-Bearbeiter/in, Art. ... StPO N. ...).

Eckert Martin, Digitale Daten als Wirtschaftsgut: digitale Daten als Sache, SJZ 112 (2016), S. 245 ff.

Forster Marc, Marksteine der Bundesgerichtspraxis zur strafprozessualen Überwachung des digitalen Fernmeldeverkehrs, in: Gschwend Lukas/Hettich Peter/Müller-Chen Markus/Schindler Benjamin/Wildhaber Isabelle (Hrsg.), Recht im digitalen Zeitalter, Festgabe Schweizerischer Juristentag 2015 in St. Gallen, Zürich/St. Gallen 2015, S. 613 ff.

Fröhlich-Bleuler Gianni, Eigentum an Daten?, Jusletter 6.3.2017.

Geiser Thomas/Wolf Stephan (Hrsg.), Basler Kommentar zum Zivilgesetzbuch II, Art. 457-977 ZGB, Art. 1-61 SchlT ZGB, 7. Aufl., Basel 2023 (zit. BSK-Bearbeiter/in, Art. ... ZGB N. ...).

Gercke Björn, Straftaten und Strafverfolgung im Internet, GA 2012, S. 474 ff.

Glassey Ludwiczak Maria, Mesures de surveillance suisses et résultats obtenus à l'étranger, Remarques à propos de l'ATF 146 IV 36, forumpoenale 5 (2020), S. 410 ff.

Gless Sabine, Beweisverbote in Fällen mit Auslandsbezug, JR 2008, S. 317 ff.

Graf Damian K. (Hrsg.), Annotierter Kommentar zum Schweizerischen Strafgesetzbuch, Bern 2020 (zit. AK-Bearbeiter/in, Art. ... StGB N. ...).

Graf Damian K., Praxishandbuch zur Siegelung, StPO inklusive revidierter Bestimmungen – VStrR – IRSG – MStP, Bern 2022 (zit. Praxishandbuch).

Graf Damian K., Strafverfolgung 2.0: Direkter Zugriff auf im Ausland gespeicherte Daten?, Jusletter IT 21.9.2017 (zit. Strafverfolgung 2.0).

Graf Jürgen-Peter (Hrsg.), BeckOK StPO mit RiStBV und MiStra, 47. Edition, München, Stand: 1.1.2023 (zit. BeckOK-Bearbeiter/in, § ... StPO N. ...).

Grassle Christian/Hiéramente Mayeul, Praxisprobleme bei der IT-Durchsuchung, CB 2019, S. 191 ff.

Grave Carsten/Barth Christoph, Von «Dawn Raids» zu «eRaids», Zu den Befugnissen der Europäischen Kommission bei der Durchsuchung elektronischer Daten, EuZW 2013, S. 360 ff.

Hansjakob Thomas, Die Erhebung von Daten des Internetverkehrs – Bemerkungen zu BGer 6B_656/2015 vom 16.12.2016, forumpoenale 4 (2017), S. 252 ff.

Heimgartner Stefan, Die internationale Dimension von Internetstraffällen, in: Schwarzenegger Christian/Arter Oliver/Jörg Florian (Hrsg.), Internet-Recht und Strafrecht, Bern 2005, S. 117 ff. (zit. Internationale Dimension).

Heimgartner Stefan, Strafprozessuale Beschlagnahme, Wesen, Arten und Wirkungen, Zürich 2011 (zit. Strafprozessuale Beschlagnahme).

Hess-Odoni Urs, Die Herrschaftsrechte an Daten, Jusletter 17.5.2004.

Hiatt Keith, Open Source Evidence on Trial, 125 Yale Law Journal Forum (2016), S. 323 ff., abrufbar unter https://www.yalelawjournal.org/pdf/Hiatt_PDF_zxz3ufoz.pdf, besucht am 17.10.2023.

Hürlimann Daniel/Zech Herbert, Rechte an Daten, sui-generis 2016, S. 89 ff., abrufbar unter <https://doi.org/10.21257/sg.27>, besucht am 17.10.2023.

Karagiannis Christos/Vergidis Kostas, Digital Evidence and Cloud Forensics: Contemporary Legal Challenges and the Power of Disposal, Information 12 (2021), 181, S. 1 ff., abrufbar unter <https://www.mdpi.com/2078-2489/12/5/181>, besucht am 17.10.2023.

Knauer Christoph/Kudlich Hans/Schneider Hartmut (Hrsg.), Münchener Kommentar zur Strafprozessordnung, Band 1: §§ 1-150 StPO, 2. Aufl., München 2022 (zit. MK-Bearbeiter/in, § ... StPO N. ...).

Kohler Patrick, Rechte an Sachdaten, sic! 2020, S. 412 ff.

Largiadèr Albert, Vorladungen ins Ausland nur Einladungen?, forumpoenale 5 (2014), S. 293 f.

Marberth-Kubicki Annette, in: Auer-Reinsdorff Astrid/Conrad Isabell (Hrsg.), Handbuch IT- und Datenschutzrecht, 2. Aufl., München 2016.

Moreillon Laurent/Parein-Reymond Aude, Petit commentaire du Code de procédure pénale, 2. Aufl., Basel 2016.

Niggli Marcel Alexander/Wiprächtiger Hans (Hrsg.), Basler Kommentar zum Strafrecht II, 4. Aufl., Basel 2019 (zit. BSK-Bearbeiter/in, Art. ... StGB N. ...).

Niggli Marcel Alexander/Heer Marianne/Wiprächtiger Hans (Hrsg.), Basler Kommentar zur Strafprozessordnung/Jugendstrafprozessordnung, 3. Aufl., Basel 2023 (zit. BSK-Bearbeiter/in, Art. ... StPO N. ...).

Obenhaus Nils, Cloud Computing als neue Herausforderung für Strafverfolgungsbehörden und Rechtsanwaltschaft, NJW 2010, S. 651 ff.

Osula Anna-Maria, Remote search and seizure in domestic criminal procedure: Estonian case study, International Journal of Law and Information Technology 24 (2016), S. 343 ff.

Pfeffer Kristin, Die Regulierung des (grenzüberschreitenden) Zugangs zu elektronischen Beweismitteln, abrufbar unter <https://eucrim.eu/articles/die-regulierung-des-grenzuberschreitenden-zugangs-zu-elektronischen-beweismitteln/>, besucht am 17.10.2023.

Riedi Claudio, *Auslandsbeweise und ihre Verwertung im schweizerischen Strafverfahren*, Zürich 2018.

Roth Simon, *Die grenzüberschreitende Edition von IP-Adressen und Bestandesdaten im Strafprozess, Direkter Zugriff oder Rechtshilfe?*, Jusletter 17.8.2015.

Ryser Dominic, «Computer Forensics», Eine neue Herausforderung für das Strafprozessrecht, in: Schwarzenegger Christian/Arter Oliver/Jörg Florian (Hrsg.), *Internet-Recht und Strafrecht*, Bern 2005, S. 553 ff.

Sampson Fraser, *Intelligence evidence: Using open source intelligence (OSINT) in criminal proceedings*, *The Police Journal* 90(1) 2017, S. 55 ff.

Schmid Alain/Schmidt Kirsten Johanna/Zech Herbert (Hrsg.), *Rechte an Daten – zum Stand der Diskussion, sic!* 11/2018, S. 627 ff.

Schmid Niklaus, *Strafprozessuale Fragen im Zusammenhang mit Computerdelikten und neuen Informationstechnologien im allgemeinen*, ZStrR 111 (1993), S. 81 ff.

Schomburg Wolfgang/Lagodny Otto (Hrsg.), *Internationale Rechtshilfe in Strafsachen*, Beck'scher Kurz-Kommentar, 6. Aufl., München 2020 (zit. Schomburg/Lagodny-Bearbeiter/in).

Schweingruber Sandra, *Cybercrime-Strafverfolgung im Konflikt mit dem Territorialitätsprinzip*, Jusletter 10.11.2014.

Seger Alexander, «Grenzüberschreitender» Zugriff auf Daten im Rahmen der Budapest Konvention über Computerkriminalität, *Praxisbericht zum Stand der Arbeiten des Europarats*, *Zeitschrift für öffentliches Recht* 73 (2018), S. 71 ff.

Seitz Nicolai, *Transborder Search: A New Perspective in Law Enforcement?*, *Yale Journal of Law & Technology* 2004-2005, S. 24 ff., abrufbar unter <https://yjolt.org/transborder-search-new-perspective-law-enforcement>, besucht am 17.10.2023.

Singelstein Tobias, *Möglichkeiten und Grenzen neuerer strafprozessualer Ermittlungsmassnahmen – Telekommunikation, Web 2.0, Datenbeschlagnahme, polizeiliche Datenverarbeitung & Co.*, NStZ 2012, S. 593 ff.

Svantesson Dan, Preliminary Report: Law Enforcement Cross-Border Access to Data, 12.11.2016, abrufbar unter <https://ssrn.com/abstract=2874238>, besucht am 17.10.2023.

Unselde Lea, Internationale Rechtshilfe im Steuerrecht, Akzessorische Rechtshilfe, Auslieferung und Vollstreckungshilfe bei Fiskaldelikten, Zürich 2011.

Velasco Cristos, Cybercrime jurisdiction: past, present, future, ERA Forum (2015) 16, S. 331 ff., abrufbar unter <https://rm.coe.int/16806b8a7a>, besucht am 17.10.2023.

Wabnitz Heinz-Bernd/Janovsky Thomas (Hrsg.), Handbuch des Wirtschafts- und Steuerstrafrechts, 4. Aufl., München 2014 (zit. Wabnitz/Janovsky-Bearbeiter/in).

Walden Ian, Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent, Queen Mary School of Law Legal Studies Research Paper No. 7 (2011), abrufbar unter <https://papers.ssrn.com/abstract=1781067>, besucht am 17.10.2023.

Walder Stephan, Grenzüberschreitende Datenerhebung: Ist und Soll, Kriminalistik 8-9/2019, S. 540 ff.

Weber Amalie M., The Council of Europe's Convention on Cybercrime, Berkeley Technology Law Journal 18 (2003), S. 425 ff., abrufbar unter <https://lawcat.berkeley.edu/record/1118718>, besucht am 17.10.2023.

Wicker Magda, Durchsuchung in der Cloud, Nutzung von Cloud-Speichern und der strafprozessuale Zugriff deutscher Ermittlungsbehörden, MMR 2013, S. 765 ff.

Zerbes Ingeborg/El-Ghazi Mohamad, Zugriff auf Computer: Von der gegenständlichen zur virtuellen Durchsuchung, NStZ 2015, S. 425 ff.

I MATERIALI

Botschaft des Bundesrates an die Bundesversammlung zu einem Bundesgesetz über internationale Rechtshilfe in Strafsachen und einem Bundesbeschluss über Vorbehalte zum Europäischen Auslieferungsübereinkommen

vom 8.3.1976, BBl 1976 II 444 ff., abrufbar unter https://www.fedlex.admin.ch/eli/fga/1976/2_444_430_443/de, besucht am 17.10.2023.

Botschaft über die Genehmigung und die Umsetzung des Übereinkommens des Europarates über die Cyberkriminalität vom 18.6.2010, BBl 2010 4697 ff., abrufbar unter <https://www.fedlex.admin.ch/eli/fga/2010/813/de>, besucht am 17.10.2023.

Botschaft zum Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) vom 27.2.2013, BBl 2013 2683 ff., abrufbar unter <https://www.fedlex.admin.ch/eli/fga/2013/512/de>, besucht am 17.10.2023.

Botschaft zur Vereinheitlichung des Strafprozessrechts vom 21.12.2005, BBl 2006 1085 ff., abrufbar unter <https://www.fedlex.admin.ch/eli/fga/2006/124/de>, besucht am 17.10.2023.

Bundesamt für Justiz, Zusammenfassung der Ergebnisse des Vernehmlassungsverfahrens zum erläuternden Bericht und zum Vorentwurf über die Änderung des Schweizerischen Strafgesetzbuches und des Rechtshilfegesetzes, Genehmigung und Umsetzung des Übereinkommens des Europarates über die Cyberkriminalität, Bern, 10.4.2010, abrufbar unter <https://www.bj.admin.ch/bj/de/home/sicherheit/gesetzgebung/archiv/cybercrime-europarat.html>, besucht am 17.10.2023.

Europäische Union, Common Position of 27 May 1999 adopted by the Council on the basis of Article 34 of the Treaty on European Union, on negotiations relating to the Draft Convention on Cyber Crime held in the Council of Europe, Official Journal of the European Communities, L 142/1 vom 5.6.1999, abrufbar unter <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1999:142:0001:0002:EN:PDF>, besucht am 17.10.2023.

Europarat, Cybercrime Convention Committee (T-CY), The Budapest Convention on Cybercrime: benefits and impact in practice, Strassburg, 13.7.2020, abrufbar unter <https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac>, besucht am 17.10.2023 (zit. T-CY, Benefits).

Europarat, Cybercrime Convention Committee (T-CY), T-CY Guidance Note # 3, Transborder access to data (Article 32), Strassburg, 3.12.2014, abrufbar unter <https://www.ccdcoe.org/uploads/2019/09/CoE-141203-Guidance-Note-on-Transborder-access-to-data.pdf>, besucht am 17.10.2023 (zit. T-CY Guidance Note # 3).

Europarat, Cybercrime Convention Committee (T-CY), Ad-hoc Sub-group on Jurisdiction and Transborder Access to Data, Transborder Access and jurisdiction: What are the options?, Strassburg, 6.12.2012, abrufbar unter <https://rm.coe.int/16802e79e8>, besucht am 17.10.2023 (zit. T-CY, Transborder Access).

Europarat, Cybercrime Convention Committee (T-CY), T-CY Cloud Evidence Group, Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY, Final report, Strassburg, 16.9.2016, abrufbar unter <https://rm.coe.int/16806a495e>, besucht am 17.10.2023 (zit. T-CY, Cloud).

Europarat, Cybercrime Convention Committee (T-CY), T-CY assessment report: The mutual legal assistance provisions of the Budapest Convention on Cybercrime, Strassburg, 3.12.2014, abrufbar unter <https://rm.coe.int/16802e726c>, besucht am 17.10.2023 (zit. T-CY, Assessment Report).

Europarat, Draft Explanatory Memorandum Regarding on Draft Recommendation No. R (95) Concerning Problems of Criminal Procedural Law Connected with Information Technology vom 31.7.1995 (zit. Explanatory Memorandum).

Europarat, Economic Crime Division, Project on Cybercrime, Cloud Computing and cybercrime investigations: Territoriality vs. the power of disposal?, Discussion Paper, Strassburg, 31.8.2010, abrufbar unter <https://rm.coe.int/16802fa3df>, besucht am 17.10.2023 (zit. Economic Crime Division).

Europarat, Explanatory Report to the Convention on Cybercrime, Budapest, 23.11.2001, abrufbar unter <https://rm.coe.int/16800cce5b>, besucht am 17.10.2023 (zit. Explanatory Report).

United Nations, Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communication Technologies for Criminal Purposes, Consolidated negotiating document on the general provisions and the provisions on criminalization and on procedural measures and law enforcement of a comprehensive international convention on countering the use of information and communications technologies for criminal purposes vom 21.1.2023, abrufbar unter https://www.unodc.org/documents/Cybercrime/AdHocCommittee/4th_Session/Documents/CND_21.01.2023_-_Copy.pdf,

besucht am 17.10.2023 (zit. United Nations, Consolidated Negotiating Document).

United Nations, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, Note by the Secretary-General vom 24.6.2013, UN Doc A/68/98, abrufbar unter <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N13/371/66/PDF/N1337166.pdf>, besucht am 17.10.2023 (zit. Developments).

United Nations Office on Drugs and Crime (UNODC), Comprehensive Study on Cybercrime, Draft February 2013, abrufbar unter https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf, besucht am 17.10.2023 (zit. UNODC).

ATTENZIONE: Questa versione del commentario è una traduzione automatica dell'originale. Il commentario originale è in francese. La traduzione è stata effettuata con www.deepl.com. Solo la versione originale fa fede. La forma tradotta del commentario non può essere citata

COMMENTO SU

Art. 33 CCC (Convenzione sulla cibercriminalità [Cybercrime Convention])

Un commentario di Nicolas Bottinelli / Julien Wenger

CITAZIONE SUGGERITA

Nicolas Bottinelli/Julien Wenger, Commentario all'art. 33 CCC, in: Damian K. Graf (a cura di), Commentario online alla Convenzione sulla cibercriminalità [Cybercrime Convention]

Breve citazione: OK-Bottinelli/Wenger, art. 33 CCC N. XXX.

Art. 33 Assistenza giudiziaria per la raccolta in tempo reale di dati relativi al traffico informatico

¹ Le Parti si forniscono reciprocamente assistenza giudiziaria per la raccolta in tempo reale di dati relativi al traffico informatico di specifiche comunicazioni effettuate sul loro territorio e trasmesse attraverso un sistema informatico. Fatte salve le disposizioni del paragrafo 2, questa assistenza è soggetta alle condizioni e alle procedure previste dal diritto interno.

² Le Parti forniscono assistenza giudiziaria almeno per i reati per i quali la raccolta in tempo reale dei dati relativi al traffico informatico sarebbe possibile in una situazione analoga a livello nazionale.

STRUTTURA

I. Introduzione	286
II. Concetti	287
III. Attuazione nel diritto svizzero	290
A. Art. 18b AIMP	290
1. Contesto	290
2. Definizioni	290
3. La procedura	291
4. Alcune delimitazioni materiali	294
B. Distinzioni	295
Bibliografia	296
I Materiali	297

I. INTRODUZIONE

- 1 Incluso nel Capitolo III della Convenzione sulla criminalità informatica intitolato "Cooperazione internazionale", l'art. 33 CCC è la prima delle due disposizioni della Convenzione che riguardano gli obblighi di cooperazione degli Stati contraenti nella raccolta e nella trasmissione di dati sulle comunicazioni. Questa disposizione riguarda i dati sul traffico, a differenza dell'art. 34 CCC, che si occupa dei dati relativi al contenuto della comunicazione.
- 2 La ratio legis di questa disposizione è che, molto spesso, gli investigatori non possono essere sicuri di risalire alla fonte di una comunicazione basandosi sulle registrazioni di trasmissioni precedenti, perché i dati cruciali sul traffico possono essere stati automaticamente cancellati da un fornitore di servizi dal percorso di trasmissione prima che potessero essere conservati; si è quindi ritenuto necessario che gli investigatori di ciascuna Parte possano ottenere in tempo reale i dati sul traffico relativi alle comunicazioni trasmesse da un sistema informatico sul territorio di altre Parti.
- 3 La prassi svizzera conferma questa necessità, vista la proliferazione di piattaforme di messaggistica e di posta elettronica che offrono servizi di anonimizzazione non solo attraverso l'uso della crittografia end-to-end, talvolta abbinata alla crittografia ad accesso zero, ma anche attraverso l'assenza di conservazione dei dati di traffico, ma anche per il fatto che non vengono conservati i log delle connessioni, in modo che né il monitoraggio retroattivo dei dati di traffico né la ricerca dei dati memorizzati possano identificare l'utente del servizio. L'intercettazione in tempo reale dei dati consente di risalire alla fonte della comunicazione, se necessario attraverso il meccanismo previsto dall'art. 30 del Codice penale.
- 4 L'articolo 33 cpv. 2, del TCC obbliga gli Stati contraenti a fornire assistenza reciproca "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". È quindi il diritto penale sostanziale nazionale (in particolare il catalogo dei reati) a definire il quadro minimo degli impegni di ciascuna Parte. Questa soluzione ha il merito di evitare l'insidia di stilare un elenco di reati per i quali dovrebbe essere concessa l'assistenza reciproca in questa costellazione, che, data la diversità delle culture e dei sistemi giuridici, avrebbe indubbiamente

suscitato le proteste di molti Stati. D'altra parte, essa mira a incoraggiare le Parti a concedere la misura più ampia possibile di assistenza giudiziaria, anche in situazioni in cui i reati perseguiti non potrebbero giustificare una tale misura di sorveglianza nei procedimenti penali nazionali, soluzione che la Svizzera non ha deciso di adottare.

A livello di diritto processuale nazionale, il CCC obbliga gli Stati contraenti ad adottare le misure legislative necessarie per consentire alle autorità competenti, da un lato, di raccogliere o registrare sul proprio territorio, in tempo reale, i dati sul traffico associati a specifiche comunicazioni trasmesse sul proprio territorio per mezzo di un sistema informatico e, dall'altro, di obbligare i fornitori di servizi a raccogliere o registrare essi stessi tali dati o ad assistere le autorità in tal senso (art. 20 CCC).

II. CONCETTI

Per "dati sul traffico", la Convenzione intende "qualsiasi dato relativo a una comunicazione che passa attraverso un sistema informatico, prodotto da quest'ultimo come parte della catena di comunicazione, che indichi l'origine, la destinazione, il percorso, l'ora, la data, la dimensione e la durata della comunicazione o il tipo di servizio sottostante" (art. 1 lett. d CDC). Questi dati sono prodotti dai computer della catena di comunicazione per instradare il contenuto di una comunicazione dall'origine alla destinazione. Sono quindi ausiliari rispetto alla comunicazione stessa. Per "origine" si intende un numero di telefono, un indirizzo IP o un mezzo simile per identificare un dispositivo di comunicazione a cui un fornitore di servizi fornisce servizi. Per "destinazione" si intende un'indicazione analoga di un dispositivo di comunicazione a cui vengono trasmesse le comunicazioni. Tipo di servizio sottostante" si riferisce al tipo di servizio utilizzato all'interno della rete: trasferimento di file, e-mail o messaggistica istantanea. In sintesi, i dati sul traffico forniscono informazioni sul mittente e sul destinatario, nonché sull'ora, l'entità, la durata, il tipo e il percorso di una comunicazione.

La definizione stessa di "dati sul traffico" non è stata espressamente ripresa dal legislatore svizzero nel contesto dell'attuazione della Convenzione (in particolare nell'articolo 18b AIMP; cfr. infra III.A.). All'epoca, il Consiglio federale ritenne che la definizione fosse sufficientemente descritta dalla dottrina e dalla prassi, ovvero: "I dati sul traffico comprendono in particolare le risorse di indirizzamento dell'origine dell'accesso, la data e l'ora di inizio e

fine della connessione, i dati utilizzati per la procedura di identificazione (login) e il tipo di connessione". Dal 1° settembre 2016, la legge svizzera definisce i "dati secondari delle telecomunicazioni" (art. 273 CPP che fa riferimento all'art. 8 lett. b LSCPT) come "dati che indicano con chi, quando, per quanto tempo e da dove la persona sorvegliata è stata o è in comunicazione, nonché le caratteristiche tecniche della comunicazione in questione". Questo concetto di dati secondari è applicabile anche alle telecomunicazioni in generale - e non solo al traffico informatico - e comprende il concetto di dati sul traffico. Questo concetto si contrappone a quello di dati di contenuto (si veda il commento all'art. 34 CCC).

- 8 L'articolo 33 CCC riguarda la raccolta in tempo reale dei dati sul traffico. L'obiettivo è intercettare questi dati, ora e in futuro, nel momento in cui le comunicazioni arrivano o partono. Questo concetto si oppone alla raccolta di dati preesistenti, registrati o memorizzati su un supporto informatico (server, cloud o altro), anche quando i dati si riferiscono al traffico di comunicazioni già avvenute. Questa temporalità diretta significa che la persona sottoposta a sorveglianza non ha alcun controllo sui dati. In altre parole, la persona interessata in genere non ha la possibilità di cancellarli prima che vengano intercettati. In linea di principio, l'"intercettazione" di questi dati viene effettuata da un fornitore terzo (fornitore di Internet e/o telefono, o un fornitore di telecomunicazioni derivato, come le società che gestiscono applicazioni di comunicazione). A nostro avviso, l'articolo 33 del Codice civile non copre l'intercettazione di dati direttamente dalla persona sottoposta a sorveglianza mediante un software "cavallo di Troia" (Govware). D'altro canto, non sembra esclusa l'intercettazione del traffico per mezzo di uno speciale dispositivo tecnico di sorveglianza, come un IMSI catcher (si veda il successivo punto III.A.3).
- 9 I dati intercettati devono essere "associati a comunicazioni specifiche". L'uso del plurale si spiega con il fatto che può essere necessario raccogliere dati sul traffico relativi a più comunicazioni per stabilire l'identità della persona che origina la comunicazione e/o della persona a cui la comunicazione è destinata. La nozione di "specificato" significa che il CCC non richiede agli Stati Parte di attuare un monitoraggio generale o sistematico e la raccolta di grandi quantità di dati sul traffico. Questa disposizione non può quindi giustificare una ricerca indeterminata di prove ("fishing expedition"). Secondo gli autori, anche i log delle connessioni a una casella e-mail (log e IP associati)

sono "associati a una comunicazione specifica" ai sensi di questa disposizione. Anche se la connessione a una casella di posta elettronica non comporta necessariamente l'invio o la ricezione di una comunicazione, è una condizione necessaria. Questo sembra essere l'approccio adottato dalla legge svizzera; infatti, come abbiamo visto, nel Messaggio CCC, il Consiglio federale si è basato su una definizione della dottrina che include le risorse di indirizzamento, comprese le date e gli orari di connessione e disconnessione. L'articolo 18b dell'AIMP non include il concetto di "comunicazioni specificate", che in particolare apre la strada alla raccolta in tempo reale e alla trasmissione anticipata dei log di connessione (cfr. *infra* III.A.4.).

Inoltre, le comunicazioni specifiche devono avvenire sul territorio di una 10 Parte. Questo aspetto potrebbe essere potenzialmente problematico, dato che l'uso di tecnologie di tipo cloud non consente più di associare un luogo di archiviazione a un particolare Stato. In pratica, il criterio del luogo di archiviazione dei dati ha perso importanza a favore del luogo in cui si trova la persona (fisica o giuridica) che ha il controllo effettivo dei dati. Secondo gli autori, l'articolo 33 del Codice civile si applica anche in questo nuovo contesto.

La disposizione prevede che le Parti si prestino reciproca assistenza nella 11 raccolta in tempo reale di tali dati. Sebbene, a una prima lettura, il concetto di "raccolta" comprenda anche quello di "trasmissione" - poiché tale raccolta avviene su richiesta e per i fini di un'autorità straniera - vedremo che il legislatore svizzero ha operato una distinzione tra questi due concetti nell'attuazione dell'articolo 33 CDC (cfr. *infra*, III).

Infine, la Convenzione non si applica in quanto tale alle telecomunicazioni 12 tradizionali (telefonia analogica), poiché i dati devono essere trasmessi mediante un sistema informatico. Tuttavia, l'avvento del telefono digitale e, più in generale, la convergenza delle tecnologie di telecomunicazione rende meno netta la distinzione tra telecomunicazioni e informatica e le caratteristiche specifiche delle loro infrastrutture. Pertanto, la Convenzione - in particolare gli articoli 20 e 33 del Codice civile - si applica a determinate comunicazioni trasmesse per mezzo di un sistema informatico, laddove la comunicazione può essere trasmessa attraverso una rete di telecomunicazioni prima di essere ricevuta da un altro sistema informatico.

III. ATTUAZIONE NEL DIRITTO SVIZZERO

A. Art. 18b AIMP

1. Contesto

- 13 L'articolo 18b EIMP è stato introdotto in seguito alla ratifica della CCC da parte della Svizzera. Il Messaggio CCC ricorda che le misure di sorveglianza in tempo reale devono, per loro stessa natura, rimanere sconosciute alle persone sorvegliate; questo postulato è difficilmente conciliabile con il principio fondamentale dell'AIMP, secondo il quale nessuna informazione relativa alla sfera segreta di una persona può essere trasmessa all'estero senza che questa abbia prima avuto la possibilità di opporsi. L'art. 18b AIMP permette quindi di soddisfare i requisiti dell'art. 33 CCC.

2. Definizioni

- 14 Ai sensi dell'art. 18b cpv. 1 AIMP, l'autorità federale o cantonale competente per l'esame di una domanda di assistenza giudiziaria può ordinare la trasmissione all'estero di dati relativi al traffico informatico prima della conclusione della procedura di assistenza giudiziaria se dalle misure provvisorie risulta che la fonte della comunicazione oggetto della domanda di assistenza giudiziaria si trova all'estero (cpv. 1 lett. a) o se la fonte della comunicazione è all'estero (cpv. 1 lett. b)). 1(a)) o se i dati sono raccolti dall'autorità di esecuzione in base a un ordine di sorveglianza in tempo reale autorizzato (artt. 269-281 del Codice di procedura penale svizzero; cpv. 2 lett. b). Mentre la lettera a è la normativa di attuazione dell'art. 30 del Codice penale, la lettera b attua gli impegni internazionali della Svizzera ai sensi dell'art. 33 del Codice penale. Tuttavia, questa disposizione non garantisce ancora la concessione dell'assistenza giudiziaria, poiché il paragrafo 2 vieta l'uso di tali dati come prova prima che la decisione sulla concessione e sulla portata dell'assistenza giudiziaria (art. 80d AIMP) sia passata in giudicato. La decisione basata sull'art. 18b EIMP che consente un rapido accesso ai dati da parte dell'autorità richiedente è una decisione accessoria, che apre la strada alla classica procedura di assistenza giudiziaria prevista dal diritto svizzero. A questo proposito, il legislatore si è preoccupato di distinguere la raccolta dei dati e il loro rapido accesso da parte dell'autorità richiedente dall'assistenza

giudiziaria vera e propria, conciliando così l'ordinamento giuridico svizzero e gli impegni internazionali.

3. La procedura

L'articolo 18b cpv.1 lettera b dell'AIMP fa riferimento agli articoli da 269 a 281 ¹⁵ del Codice penale svizzero e quindi, in particolare, nel caso della sorveglianza dei dati secondari delle telecomunicazioni, all'articolo 273 del Codice penale svizzero. Quest'ultimo prevede in particolare che solo i gravi sospetti sulla commissione di crimini e delitti (art. 10 cpv. 2 e 3 CP) consentono al pubblico ministero di ottenere dati secondari di telecomunicazione. Pertanto, il legislatore svizzero non ha voluto aprire il campo di applicazione dell'articolo 33 CP a reati che non consentirebbero l'applicazione di tali misure secondo il diritto svizzero, come proposto dall'articolo 33 cpv. 2 CP.

L'art. 18b cpv. 1 lett. b AIMP costituisce una deroga al sistema classico di ¹⁶ assistenza giudiziaria, in base al quale deve essere garantito il diritto di essere ascoltato della persona interessata da una misura di assistenza giudiziaria e deve essere debitamente notificato ed entrato in vigore un ordine di chiusura prima di qualsiasi trasmissione di prove all'estero (art. 80d AIMP). Prima dell'entrata in vigore di questa disposizione, la Svizzera non poteva fornire tali dati segreti di sorveglianza all'estero senza informare preventivamente la persona interessata (a condizione che fosse domiciliata in Svizzera o che vi avesse eletto domicilio; cfr. art. 80m AIMP), il che significava che la misura era spesso inutile per il procedimento estero, e poteva addirittura comprometterlo.

D'ora in poi, una volta presa una decisione (art. 80a AIMP), l'autorità di ¹⁷ esecuzione ordinerà la misura di sorveglianza attraverso il Service Surveillance de la correspondance par poste et télécommunication (Service SCPT; art. 273 CPP in combinato disposto con l'art. 60 ss. OSCPT).

L'autorità deve poi ottenere l'autorizzazione alla misura dal Tribunale per i ¹⁸ provvedimenti coercitivi entro 24 ore dall'ordine (art. 274 cpv. 1 CPP). Va notato che, per quanto riguarda la condizione, prevista dall'art. 273 del Codice di procedura penale svizzero, dell'esistenza di un "grave sospetto", il Tribunale federale ha giustamente sottolineato che, secondo le norme sull'assistenza giudiziaria e la giurisprudenza consolidata, gli articoli 14 della CGCE, 28 dell'AIMP e 10 dell'AIMP impongono all'autorità richiedente di spiegare in

cosa consistono i suoi sospetti, ma non di provarli o anche solo di renderli probabili. Fatto salvo il divieto di richieste esplorative, i sospetti dell'autorità richiedente non devono quindi essere particolarmente gravi o precisi. Sebbene il diritto interno debba essere applicato quando è più favorevole alla cooperazione rispetto al diritto dei trattati, esso non può imporre condizioni materiali all'assistenza reciproca che non siano previste dal diritto dei trattati.

- 19 Il Tribunale per le misure coercitive si pronuncia entro cinque giorni (art. 274 cpv. 2 CPP). Se la sorveglianza viene rifiutata, i documenti e le registrazioni raccolti devono essere distrutti immediatamente (art. 277 cpv. 1 CPP). Se l'autorizzazione viene concessa, va notato che l'art. 279 del Codice di procedura penale svizzero (CCP), che prevede la comunicazione all'imputato o al terzo oggetto della sorveglianza e stabilisce un diritto di ricorso per loro e per il servizio di telecomunicazione sorvegliato (art. 279 cpv. 3 CCP), non si applica, nonostante il riferimento dell'art. 18b cpv. 2 lett. a agli artt. 269-281 CCP. Questo perché le convenzioni e le leggi applicabili nel campo dell'assistenza giudiziaria internazionale in materia penale derogano al sistema abituale del Codice di procedura penale svizzero, che si applica solo se è più favorevole alla cooperazione rispetto alle convenzioni e alle leggi applicabili (principio di favore). In particolare, ciò significa che lo status di parte, il diritto di notifica e i rimedi giuridici sono disciplinati dalle disposizioni specifiche sull'assistenza giudiziaria. Ai sensi dell'art. 80m cpv. 1 dell'EIMP, l'obbligo di notifica delle decisioni di assistenza giudiziaria è limitato alle persone che risiedono o hanno eletto domicilio in Svizzera. Qualsiasi indicazione contraria da parte dell'MCCT, sia attraverso un riferimento alla legge sia imponendo condizioni ai sensi dell'art. 274 cpv. 2 del Codice di procedura penale svizzero, sarebbe pertanto nulla, in quanto l'MCCT non è competente per questo aspetto del procedimento. Spetterà all'autorità di esecuzione, nell'ambito della procedura di assistenza giudiziaria - ossia, se del caso, dopo la trasmissione anticipata prevista dall'art. 18b AIMP - garantire il rispetto di queste convenzioni e delle leggi applicabili e fare solo le notifiche previste dall'art. 80m AIMP.
- 20 Al ricevimento dei dati di monitoraggio, l'autorità di controllo può emettere una decisione incidentale basata sull'art. 18b AIMP che ordina la trasmissione anticipata dei dati all'autorità richiedente. La decisione, così come l'ordine di sorveglianza e l'autorizzazione, saranno comunicati all'UFG (art. 18b cpv. 3 EIMP). Se la sorveglianza è destinata a durare nel tempo e i dati sono raccolti

regolarmente, la decisione può riguardare tutti i dati futuri derivanti dalla sorveglianza autorizzata, in modo da consentire all'autorità di esecuzione (o alla polizia, se del caso) di trasmettere i dati man mano che li riceve. In assenza di notifica all'interessato in questa fase e in considerazione dei limiti imposti dall'articolo 18ter cpv. 2 dell'AIMP, tale procedura non pregiudica i diritti delle parti della procedura di assistenza giudiziaria e deve essere consentita.

Tuttavia, al momento di ogni trasmissione anticipata all'autorità richiedente, 21 occorre tenere presente che tali dati non possono essere utilizzati come prova fino a quando la decisione sulla concessione e sulla portata dell'assistenza giudiziaria non sia passata in giudicato (art. 18b par. 2 AIMP). In questo modo, la protezione giuridica è garantita a posteriori. È inoltre essenziale tenere un registro - almeno sotto forma di elenco - dei dati trasmessi in anticipo, in modo che l'autorità di esecuzione, al termine della procedura di assistenza reciproca, sappia con precisione quali dati saranno oggetto della decisione finale di chiusura.

In pratica, quando la persona interessata dalla misura di sorveglianza è 22 sconosciuta, non è domiciliata in Svizzera o non vi ha eletto domicilio, o addirittura utilizza una falsa identità, l'autorità di esecuzione può convalidare rapidamente l'uso dei dati come prova mediante una decisione di chiusura. Poiché questa decisione viene notificata solo all'UFG (art. 80h lett. a EIMP), la segretezza sull'esistenza delle misure è preservata.

Se la persona interessata dalla misura di sorveglianza è domiciliata in Svizzera 23 o vi ha eletto domicilio, deve essere garantito il suo diritto di essere ascoltata (art. 80m cpv. 1 AIMP in combinato disposto con l'art. 80b AIMP), il che significa che deve essere informata della misura e avere la possibilità di esprimersi per iscritto prima dell'emissione della decisione di chiusura. L'articolo 18b dell'EIMP consente di posticipare l'informazione della persona interessata e il suo diritto di essere ascoltata per il tempo necessario alla procedura all'estero. In pratica, l'autorità di esecuzione dovrà regolarmente chiedere all'autorità richiedente se è necessario, per il procedimento all'estero, mantenere segreta la misura di sorveglianza ordinata in Svizzera.

La decisione di chiusura del procedimento può essere impugnata presso il 24 Tribunale penale federale (art. 80e AIMP). La decisione incidentale di trasmettere i dati sul traffico ai sensi dell'art. 18b AIMP può essere impugnata

contestualmente alla decisione di archiviazione (art. 80e cpv. 1 AIMP). Un ricorso immediato contro la decisione incidentale sembra possibile, se l'autorità di controllo non ha preso le precauzioni necessarie per garantire il rispetto dei requisiti dell'art. 18b par. 2 AIMP. Il ricorso al Tribunale federale rimane possibile alle condizioni restrittive dell'art. 84 dell'AFC (caso particolarmente importante). Alcuni giuristi sostengono che se il ricorso viene accolto, le informazioni trasmesse devono essere eliminate dall'archivio straniero. Questo è certamente il caso se l'autorità straniera si è impegnata a farlo, anche se questo obbligo non compare nell'art. 18b EIMP.

- 25 La formulazione molto ampia dell'articolo 18b cpv. 1, lettera b) dell'AIMP sembrerebbe consentire anche la trasmissione anticipata di dati relativi al traffico informatico qualora tali dati siano stati intercettati mediante un captatore IMSI (articolo 269bis CPP), un govware (articolo 269ter CPP) o altri dispositivi tecnici di sorveglianza (articolo 280 CPP), anche se l'articolo 33 CPC non impone tale obbligo.

4. Alcune delimitazioni materiali

- 26 A differenza del testo dell'art. 33 CPC, l'art. 18b AIMP non si limita alle "comunicazioni specificate". Ad esempio, i log delle connessioni a una casella di posta elettronica possono essere ottenuti mediante un monitoraggio in tempo reale e trasmessi in anticipo all'autorità richiedente, anche se non vi è alcuna comunicazione (ad esempio, nessuna e-mail inviata durante quella sessione di connessione o nessuna e-mail ricevuta).
- 27 Il Tribunale federale ha ritenuto che l'articolo 18 ter dell'AIMP costituisca una base giuridica per il trasferimento anticipato dei dati sul traffico derivanti dalla sorveglianza in tempo reale, a esclusione dei dati sul contenuto, in assenza di una base giuridica o contrattuale.
- 28 Nella stessa sentenza, il Tribunale federale ha aperto il trasferimento anticipato di dati ai sensi dell'articolo 18b AIMP ai dati relativi al traffico telefonico. Di conseguenza, i dati secondari derivanti dal monitoraggio attivo di una connessione telefonica (ad esempio, i numeri chiamati o chiamanti, la durata della conversazione telefonica o l'antenna attivata) sono dati che dovrebbero poter essere trasmessi in anticipo a un'autorità straniera sulla base dell'articolo 18 ter dell'AIMP. A nostro avviso, questa interpretazione del Tribunale federale è del tutto logica alla luce della diffusa digitalizzazione dei

sistemi di telecomunicazione e, di conseguenza, della natura sempre più obsoleta e artificiale della distinzione tra sistemi di telecomunicazione tradizionali da un lato e sistemi informatici dall'altro.

L'articolo 18b AIMP presenta un altro vantaggio: se la raccolta di dati sul traffico trasmessi in anticipo consente di stabilire che una nuova misura di sorveglianza su un altro conto, un'altra linea, ecc. in Svizzera o all'estero, è giustificata, l'autorità richiedente può chiedere immediatamente l'esecuzione di tale misura.

B. Distinzioni

La trasmissione anticipata di informazioni relative al traffico informatico prevista dall'articolo 18b AIMP deve essere distinta dalla trasmissione spontanea di prove e informazioni (articolo 67a AIMP), che costituisce anch'essa un'eccezione al principio secondo cui è necessaria una decisione finale prima di qualsiasi trasmissione all'estero. A differenza del sistema previsto dall'art. 67a AIMP, l'art. 18b AIMP entra necessariamente in gioco nel contesto dell'esecuzione di una richiesta estera di assistenza giudiziaria finalizzata all'ottenimento di questi mezzi di prova. L'articolo 18b AIMP non prevede la trasmissione anticipata "spontanea" dei dati sul traffico. Inoltre, l'articolo 67a AIMP vieta la trasmissione di prove non appena queste rientrano nella sfera del segreto (articolo 67 cpv. 4 AIMP). In questo caso, solo le informazioni possono essere fornite a un'autorità straniera (art. 67a cpv. 5 AIMP).

Anche la trasmissione anticipata di informazioni relative al traffico informatico ai sensi dell'art. 18b AIMP deve essere distinta dall'assistenza reciproca dinamica (art. 80dbis AIMP) che consente, in via eccezionale, la trasmissione anticipata di informazioni o prove (a) quando le indagini estere sulla criminalità organizzata o sul terrorismo sarebbero eccessivamente difficili senza questa misura di assistenza reciproca, in particolare a causa del rischio di collusione o perché deve essere preservata la riservatezza del procedimento, o (b) al fine di prevenire un pericolo grave e imminente, in particolare la commissione di un atto terroristico. L'introduzione nel 2021 di questa nuova disposizione - accompagnata da nuove norme sulla squadra investigativa comune - è stata considerata un primo passo importante verso norme più flessibili e un'assistenza reciproca più rapida e reattiva, basata sulla fiducia internazionale. Dal punto di vista dell'ambito di applicazione

materiale, l'art. 18b dell'AIMP non ha limitazioni, mentre l'art. 80dbis dell'AIMP è limitato alla criminalità organizzata e al terrorismo, tranne nei casi di pericolo grave e imminente. Per contro, l'art. 80dbis AIMP prevede che qualsiasi tipo di prova o informazione possa essere trasmessa in anticipo con questo mezzo, mentre l'ambito di applicazione dell'art. 18b AIMP è limitato esclusivamente ai dati relativi al traffico informatico, anche se va ricordato che il Tribunale federale ha aperto la strada a un'applicazione analoga dell'art. 18b AIMP in relazione alla sorveglianza telefonica. Infine, l'art. 18b AIMP non prevede - almeno esplicitamente - alcun impegno preventivo da parte dell'autorità richiedente, che deve essere informata dall'autorità di esecuzione che i dati trasmessi in anticipo non possono essere utilizzati come prova fino a quando la decisione sulla concessione e sulla portata dell'assistenza giudiziaria non sarà diventata definitiva (art. 18b cpv. 2 AIMP). Su questo punto, l'art. 80dbis AIMP è più formalistico (cfr. art. 80dbis par. 4 AIMP).

- 32 Infine, la trasmissione anticipata ai sensi dell'art. 18b AIMP non sembra essere di particolare interesse nel contesto di una squadra investigativa comune (SIC; artt. 80dter a 80dduodecies AIMP); infatti, il ristretto ambito materiale dell'art. 80dbis AIMP non si applica, secondo gli autori, alle squadre investigative comuni, nonostante l'infelice riferimento nell'art. 80docties AIMP alle condizioni dell'art. 80dbis AIMP.

Gli autori hanno scritto questo contributo a titolo personale. Le valutazioni e le opinioni presentate sono proprie e non sono vincolanti per il Ministero pubblico della Confederazione.

BIBLIOGRAFIA

Böhi Simon, commentaire de l'art. 18b EIMP, in : Niggli Marcel Alexander/Heimgartner Stefan (édit.), Basler Kommentar Internationales Strafrecht, 1^{ère} édition, Bâle 2015.

Dangubic Miro/Clerc Yves, Art. 80d^{bis} IRSG – ein Überblick, forumpoenale 4 (2022) p. 287.

Donatsch Andreas/Heimgartner Stefan/Meyer Frank/Simonek Madeleine, Internationale Rechtshilfe, 2e édition., Zurich et al. 2015.

Glutz Alexander M., commentaire de l'art. 67a EIMP, in : Niggli Marcel Alexander/Heimgartner Stefan (édit.), Basler Kommentar Internationales Strafrecht, 1^{ère} édition, Bâle 2015.

Hansjakob Thomas/Pajarola Umberto, commentaire de l'art. 272 CPP, in : Donatsch Andreas/Lieber Viktor/ Summers Sarah/Wohlers Wolfgang (édit.), Kommentar zur Schweizerischen Strafprozessordnung StPO, 3^e édition, Zurich 2020.

Isenring Bernhard/Maybud Roy D./Quiblier Laura, Phänomen Cybercrime – Herausforderungen und Grenzen des Straf- und Strafprozessrechts im Überblick, SJZ 115 (2019) p. 439.

Ludwiczak Glassey Maria/Bonzanigo Francesca, L'artificielle distinction entre « informations » et « moyens de preuve » en entraide pénale internationale, Revue Pénale Suisse 140/2022 p. 402-427.

Ludwiczak Maria, L'entraide pénale internationale 'dynamique' en bref. Le projet, les débats, le compromis, Pratique juridique actuelle, 1 (2021) p. 71–75.

Zimmermann Robert, La coopération judiciaire internationale en matière pénale, 5^e édition, Berne 2019.

I MATERIALI

Message concernant la loi fédérale sur la surveillance de la correspondance par poste et télécommunication (LSCPT) du 27 février 2013, FF 2013 2379, consultable sous <https://www.fedlex.admin.ch/filestore/fedlex.data.admin.ch/eli/fga/2013/512/fr/pdf-a/fedlex-data-admin-ch-eli-fga-2013-512-fr-pdf-a.pdf>, consulté en janvier 2024 (cité : Message LSCPT).

Message relatif à l'approbation et à la mise en œuvre de la Convention du Conseil de l'Europe sur la cibercriminalité du 18 juin 2010, FF 2010 4275, consultable sous <https://www.fedlex.admin.ch/filestore/fedlex.data.admin.ch/eli/fga/2010/813/fr/pdf-a/fedlex-data-admin-ch-eli-fga-2010-813-fr-pdf-a.pdf>, consulté en janvier 2024 (cité : Message CCC).

Rapport explicatif de la Convention sur la cibercriminalité du 23 novembre 2001, Conseil de l'Europe, Série des traités européens – no 185, consultable sous <https://rm.coe.int/16800ccea4>, consulté en janvier 2024 (cité : Rapport explicatif du Conseil de l'Europe).

ATTENZIONE: Questa versione del commentario è una traduzione automatica dell'originale. Il commentario originale è in francese. La traduzione è stata effettuata con www.deepl.com. Solo la versione originale fa fede. La forma tradotta del commentario non può essere citata

COMMENTO SU

Art. 34 CCC (Convenzione sulla cybercriminalità [Cybercrime Convention])

Un commentario di Nicolas Bottinelli / Julien Wenger

CITAZIONE SUGGERITA

Nicolas Bottinelli/Julien Wenger, Commentario all'art. 34 CCC, in: Damian K. Graf (a cura di), Commentario online alla Convenzione sulla cybercriminalità [Cybercrime Convention]

Breve citazione: OK-Bottinelli/Wenger, art. 34 CCC N. XXX.

Art. 34 Assistenza giudiziaria per l'intercettazione di dati relativi al contenuto

Nella misura consentita dai trattati e dalle leggi nazionali applicabili, le Parti si forniscono reciprocamente assistenza giudiziaria per la raccolta o la registrazione in tempo reale di dati relativi al contenuto di specifiche comunicazioni trasmesse attraverso un sistema informatico.

STRUTTURA

I. Introduzione 301

II. Nozioni..... 301

III. Attuazione nel diritto svizzero 304

 A. Intercettazione di dati sui contenuti nel diritto svizzero 304

 B. Distinzioni e casi speciali..... 307

 1. Trasmissione anticipata di dati sui contenuti? 307

 2. Distinzione tra ordine di deposito (art. 265 del Codice di procedura penale) e
misura di sorveglianza (art. 269 e segg. del Codice di procedura penale), in
particolare per quanto riguarda le caselle e-mail 308

 3. Uso di una falsa identità 309

Bibliografia 310

I Materiali 310

I. INTRODUZIONE

Parte del Capitolo III della Convenzione sulla criminalità informatica, 1 intitolato "Cooperazione internazionale", l'articolo 34 CCC tratta la cooperazione internazionale in relazione ai dati sul contenuto, in contrapposizione ai dati sul traffico, che sono trattati nell'articolo 33 CCC.

Il CCC riconosce l'importanza di poter intercettare i dati sul contenuto ai fini 2 dei procedimenti penali nazionali (art. 21 CCC): la raccolta di dati sul contenuto delle telecomunicazioni è sempre stata un utile strumento investigativo per determinare se una comunicazione è illegale e per fornire prove di reati passati o futuri. Le comunicazioni informatiche possono costituire o provare lo stesso tipo di reato, pur offrendo maggiori possibilità grazie alla trasmissione di grandi quantità di dati (testi, immagini e suoni). Non è possibile determinare in tempo reale la natura dannosa e illegale di queste comunicazioni senza intercettare il contenuto del messaggio. Se non potessero accertare e prevenire la commissione di reati nel momento in cui si verificano, le autorità di contrasto si ridurrebbero a indagare su reati passati, dove il danno è già stato fatto. Ne consegue che l'intercettazione in tempo reale dei dati relativi al contenuto delle comunicazioni informatiche è almeno, se non più, importante dell'intercettazione in tempo reale delle telecomunicazioni.

Tuttavia, l'articolo 34 del CCC non impone alcun obbligo agli Stati contraenti 3 di cooperare nella raccolta transfrontaliera di tali dati; al massimo, la relazione esplicativa del Consiglio d'Europa fa riferimento alle buone prassi stabilite nella raccomandazione del 1985 sull'applicazione del CECJ alla sorveglianza delle telecomunicazioni. Il secondo Protocollo aggiuntivo al CCC, del 12 maggio 2022, non tratta questa misura, né i lavori preparatori per il terzo Protocollo aggiuntivo al CCEJ.

II. NOZIONI

L'articolo 34 del TCC prevede che le Parti si prestino reciproca assistenza in 4 questo contesto "nella misura consentita dai rispettivi trattati e leggi nazionali applicabili". A differenza dell'articolo 33 del TCC, che si applica ai dati relativi al traffico informatico, l'articolo 34 del TCC non impone agli Stati contraenti un obbligo rigoroso di assistenza reciproca per quanto riguarda

l'intercettazione di dati relativi al contenuto delle comunicazioni informatiche. La decisione di affidarsi ai regimi e alle legislazioni nazionali era giustificata dalla natura altamente intrusiva delle intercettazioni e dal fatto che l'assistenza reciproca in questo settore era ancora agli inizi.

- 5 Il concetto di "dati relativi al contenuto" non è definito nella Convenzione. Si riferisce al contenuto informativo della comunicazione, ossia al significato della comunicazione o al messaggio o all'informazione trasmessa dalla comunicazione (diversi dai dati sul traffico). In concreto, i "dati di contenuto" si riferiscono alla comunicazione stessa, al suo oggetto, cioè in particolare al testo di un'e-mail (compreso il design svizzero della sezione "oggetto"), a un messaggio istantaneo, a eventuali allegati o al file o al flusso audio e/o video trasmesso. Questo concetto si contrappone a quello di "dati sul traffico", che comprende essenzialmente gli elementi della catena di comunicazione (origine, destinazione, percorso, ora, data, dimensione e durata della comunicazione o il tipo di servizio sottostante; art. 1 let. d CCC). Questa distinzione è fondamentale in termini di misure di sorveglianza e ha conseguenze dirette sulla concessione dell'assistenza giudiziaria internazionale. Ad esempio, a determinate condizioni, la Svizzera consente la trasmissione rapida e anticipata di dati relativi al traffico informatico sulla base dell'articolo 18b AIMP, che è escluso nel caso di dati relativi ai contenuti (cfr. III.B.1.).
- 6 L'articolo 34 del Codice penale contempla l'"intercettazione in tempo reale", un concetto che si contrappone alla ricerca di dati registrati o memorizzati su un supporto informatico (server, cloud o altro). Questa temporalità diretta implica che la persona sottoposta a sorveglianza non ha alcun controllo sui dati. In altre parole, la persona sottoposta a sorveglianza non ha la possibilità di cancellare i dati prima che vengano intercettati. In linea di principio, l'"intercettazione" di questi dati viene effettuata da un fornitore terzo (provider di Internet e/o telefono, fornitori di servizi di comunicazione derivati [di seguito: DSP], come le società che gestiscono applicazioni di comunicazione). A nostro avviso, l'art. 34 CCC non contempla in particolare l'intercettazione di dati di contenuto direttamente dal sospettato dell'indagine per mezzo di un software "cavallo di Troia" (Govware); tuttavia, nulla osta a che l'art. 34 CCC sia utilizzato come base per l'intercettazione di comunicazioni per mezzo di un IMSI Catcher.

La disposizione stabilisce che l'assistenza reciproca è concessa per la "raccolta 7 o la registrazione" di dati in tempo reale. A nostro avviso, anche se la distinzione tra questi due termini sembra poco chiara, la raccolta riguarda l'atto iniziale della raccolta dei dati, mentre la registrazione riguarda la loro memorizzazione in vista della trasmissione all'autorità richiedente o del loro utilizzo nell'indagine penale. Questi due concetti costituiscono quindi due fasi successive necessarie per l'esecuzione della sorveglianza, ma la loro distinzione ha uno scarso significato pratico. Inoltre, sebbene a una prima lettura i concetti di "raccolta" e "registrazione" includano quello di "trasmissione" - poiché tale raccolta avviene su richiesta e per gli scopi di un'autorità straniera - vedremo che il legislatore svizzero ha operato una distinzione tra questi concetti. Infatti, i dati raccolti in esecuzione di una richiesta di assistenza giudiziaria estera non sono esenti dalla consueta procedura di assistenza giudiziaria prima di qualsiasi trasmissione delle prove all'estero (cfr. in particolare infra III.A. ad art. 18a AIMP).

I dati intercettati devono essere collegati a "comunicazioni specifiche". Questo 8 termine va inteso nel senso che la Convenzione non richiede né autorizza la sorveglianza generale o sistematica e la raccolta di grandi quantità di dati relativi al contenuto (sorveglianza di massa). Non autorizza neppure le "spedizioni di pesca" nella speranza di scoprire attività criminali, che sono molto diverse dalle indagini su casi specifici di condotta illecita. Ovviamente, questo termine non significa che sia necessario determinare quali specifiche comunicazioni future tra diversi sistemi informatici dovranno essere monitorate, poiché solo raramente è possibile anticipare le comunicazioni future. Occorre tuttavia tenere presente che l'oggetto della sorveglianza (indirizzo e-mail, ID utente di un'applicazione di messaggistica, ecc.) deve essere determinato con precisione.

Infine, la Convenzione non si applica in quanto tale alle telecomunicazioni 9 tradizionali (telefonia analogica), poiché i dati devono essere trasmessi tramite un sistema informatico. Tuttavia, l'avvento del telefono digitale e, più in generale, la convergenza delle tecnologie di telecomunicazione rende meno netta la distinzione tra telecomunicazioni e teleinformatica e le caratteristiche specifiche delle loro infrastrutture. Pertanto, la Convenzione - in particolare gli articoli 21 e 34 del Codice civile - si applica alle comunicazioni specifiche trasmesse per mezzo di un sistema informatico, laddove la comunicazione

può essere trasmessa attraverso una rete di telecomunicazioni prima di essere ricevuta da un altro sistema informatico.

III. ATTUAZIONE NEL DIRITTO SVIZZERO

A. Intercettazione di dati sui contenuti nel diritto svizzero

- 10 Mentre l'articolo 33 del Codice penale ha portato all'introduzione dell'articolo 18b dell'AIMP, che consente di trasmettere all'autorità richiedente i dati relativi al traffico informatico in anticipo (ossia prima dell'entrata in vigore di una decisione di chiusura), l'articolo 34 del Codice penale non ha portato - almeno direttamente - ad alcun cambiamento nella legislazione svizzera sull'intercettazione dei dati relativi al contenuto. Pertanto, si applicano le consuete regole della procedura penale svizzera (art. 269 e seguenti del Codice penale svizzero), con alcune riserve, in riferimento all'art. 18a AIMP.
- 11 L'articolo 18a AIMP è la disposizione chiave relativa alla sorveglianza della corrispondenza postale e delle telecomunicazioni nel contesto dell'assistenza giudiziaria. In sostanza, stabilisce che, su esplicita richiesta di un'autorità richiedente, la Procura - e in alcuni casi anche l'Ufficio federale di giustizia - può ordinare tale sorveglianza (cpv. 2) e che l'ordine deve essere sottoposto all'approvazione del Tribunale dei provvedimenti coercitivi competente (cpv. 3). Per il resto, l'art. 18a AIMP rimanda agli articoli 269-279 CPP e alla Legge federale del 6 ottobre 2000 sulla sorveglianza della corrispondenza postale e delle telecomunicazioni (LSCPT). Questo riferimento agli articoli 269 e seguenti del Codice penale - in particolare all'elenco dei reati di cui all'articolo 269 del Codice penale - corrisponde alla "gamma di reati gravi" che le Parti devono definire nel loro diritto interno per consentire l'intercettazione dei dati sul contenuto (articoli 21 e 34 del Codice penale). Il riferimento generale alle disposizioni della LSCPT permette inoltre di ritenere che l'articolo 18a AIMP si applichi sia alle comunicazioni ordinarie (telefonia analogica tradizionale) sia alle comunicazioni collegate a un sistema informatico (cfr. in particolare l'articolo 2 cpv. c LSCPT).
- 12 In pratica, dopo essere entrata in materia (art. 80a AIMP), l'autorità di esecuzione ordinerà la misura di sorveglianza attraverso il Service Surveillance de la correspondance par poste et télécommunication (di seguito: Service SCPT; art. 269 CPP in relazione all'art. 55 ss. OSCPT). Sarà quindi possibile ordinare il monitoraggio in tempo reale del contenuto e dei

dati secondari dei servizi di accesso alla rete (art. 55 OSCPT), il monitoraggio in tempo reale del contenuto e dei dati secondari dei servizi di telefonia e multimediali (art. 57 OSCPT) o il monitoraggio in tempo reale del contenuto e dei dati secondari dei servizi di posta elettronica (art. 59 OSCPT).

L'autorità di esecuzione deve quindi ottenere l'autorizzazione del provvedimento dal Tribunale dei provvedimenti coercitivi entro 24 ore dall'ordine (art. 274 cpv. 1 CPP). Va notato che, per quanto riguarda la condizione dell'esistenza di un "grave sospetto" di cui all'art. 269 cpv. 1 lett. a del Codice di procedura penale svizzero, il Tribunale federale ha giustamente sottolineato che, secondo le norme sull'assistenza giudiziaria e la giurisprudenza consolidata, gli artt. 14 CGE, 28 AIMP e 10 AIMP impongono all'autorità richiedente di spiegare in cosa consistano i suoi sospetti, ma non di provarli o anche solo di renderli probabili. Fatto salvo il divieto di richieste esplorative, i sospetti dell'autorità richiedente non devono quindi essere particolarmente gravi o precisi. Sebbene il diritto interno debba essere applicato quando è più favorevole alla cooperazione rispetto al diritto dei trattati, non può stabilire condizioni materiali per l'assistenza reciproca che non siano previste dal diritto dei trattati. 13

Il Tribunale per le misure coercitive si pronuncia entro cinque giorni (art. 274 cpv. 2 CPP). Se la sorveglianza viene rifiutata, i documenti e le registrazioni raccolti devono essere distrutti immediatamente (art. 277 cpv. 1 CPP). Se l'autorizzazione viene concessa, va notato che l'art. 279 del Codice di procedura penale svizzero (CCP), che prevede la divulgazione all'imputato o al terzo oggetto della sorveglianza e stabilisce un diritto di ricorso per loro e per il servizio di telecomunicazione sorvegliato (art. 279 cpv. 3 CCP), non si applica, nonostante il riferimento dell'art. 18a cpv. 4 AIMP agli artt. 269-279 CCP. Ciò è dovuto al fatto che le convenzioni e le leggi applicabili all'assistenza giudiziaria internazionale in materia penale derogano al sistema abituale del Codice di procedura penale svizzero, che si applica solo se è più favorevole alla cooperazione rispetto alle convenzioni e alle leggi applicabili (principio del favor rei). In particolare, ciò significa che lo status di parte, il diritto di notifica e i rimedi giuridici sono disciplinati dalle disposizioni specifiche sull'assistenza giudiziaria. Ai sensi dell'art. 80m cpv. 1 dell'EIMP, l'obbligo di notifica delle decisioni di assistenza giudiziaria è limitato alle persone che risiedono o hanno eletto domicilio in Svizzera. Qualsiasi indicazione contraria da parte dell'MCCT, sia attraverso un riferimento alla 14

legge sia imponendo condizioni ai sensi dell'art. 274 cpv. 2 del Codice di procedura penale svizzero, sarebbe pertanto nulla, in quanto l'MCCT non è competente per questo aspetto del procedimento. Spetterà all'autorità di esecuzione, nell'ambito della procedura di assistenza giudiziaria, garantire il rispetto di queste convenzioni e delle leggi applicabili ed effettuare le notifiche previste dall'art. 80m AIMP.

- 15 Una volta ricevuti i dati di sorveglianza, l'autorità di esecuzione deve garantire il diritto di essere ascoltata alla persona interessata dalla misura di sorveglianza (art. 80b EIMP). Si vedrà che, nel caso di dati relativi al contenuto, qualsiasi trasmissione anticipata, cioè prima dell'entrata in vigore di una decisione di chiusura, è in linea di principio esclusa (si veda il successivo punto III.B.1.). Poiché la misura coercitiva in questione è essenzialmente segreta, la sua divulgazione all'interessato può avere gravi conseguenze per il procedimento all'estero. Occorre distinguere tra due situazioni:

1. Se la persona interessata dalla misura non è domiciliata in Svizzera o non vi ha eletto domicilio, la decisione dell'autorità non deve esserle notificata (art. 80m cpv. 1 AIMP). La decisione di chiusura sarà notificata solo all'UFG (art. 80h lett. a EIMP), il che significa che i risultati della vigilanza possono essere trasmessi all'autorità richiedente senza che la persona interessata sia stata effettivamente informata. Naturalmente, se l'interessato si rivolge all'autorità di esecuzione e ha eletto domicilio in Svizzera prima dell'entrata in vigore della decisione di chiusura, deve essere garantito il suo diritto a partecipare alla procedura e ad accedere al fascicolo (art. 80b cpv. 1 in combinato disposto con l'art. 80m cpv. 2 AIMP).

2. Se la persona oggetto del provvedimento è domiciliata in Svizzera o vi ha eletto domicilio, l'autorità di esecuzione deve garantirle il diritto di partecipare al procedimento e di consultare il fascicolo (art. 80b cpv. 1 AIMP; fatto salvo il caso specifico dell'uso di una falsa identità, cfr. infra III.B.3) prima di qualsiasi trasmissione dei mezzi di prova all'estero. Tuttavia, nulla obbliga l'autorità richiedente a concedere questo diritto alla persona interessata non appena la misura di sorveglianza è terminata. La misura può rimanere segreta per tutto il tempo necessario al procedimento all'estero. L'autorità di esecuzione dovrà accertarsi presso l'autorità richiedente quando l'esistenza della misura di sorveglianza potrà essere rivelata per consentire la prosecuzione della procedura di assistenza giudiziaria.

Al termine della procedura, l'autorità di esecuzione emette una decisione di chiusura che può essere impugnata presso il Tribunale penale federale (art. 80e AIMP). Un successivo ricorso al Tribunale federale rimane possibile alle condizioni restrittive dell'art. 84 dell'AFC (caso di particolare importanza). 16

B. Distinzioni e casi speciali

1. Trasmissione anticipata di dati sui contenuti?

A determinate condizioni, l'art. 18b AIMP consente la trasmissione anticipata - cioè prima dell'emissione di una decisione di chiusura - dei dati relativi al traffico informatico raccolti nell'ambito di un ordine di sorveglianza in tempo reale autorizzato. L'articolo 18b AIMP attua gli obblighi derivanti dall'articolo 33 del Codice penale. Nel caso dei dati sui contenuti, tuttavia, il Tribunale federale ha confermato che l'art. 18b EIMP non si applica e che, di conseguenza, qualsiasi trasmissione anticipata, cioè prima dell'entrata in vigore di una decisione di chiusura, è esclusa sulla base di questa disposizione. La Svizzera viene così privata di un importante strumento nella lotta alla criminalità internazionale, in particolare alla criminalità organizzata e al terrorismo. È inoltre discutibile se, con questa interpretazione del Tribunale federale, l'articolo 18a dell'AIMP abbia ancora una reale portata e utilità pratica. 17

Nel 2021, tuttavia, il legislatore ha introdotto nuove disposizioni che compensano in parte questa lacuna e costituiscono un passo importante verso regole più flessibili e un'assistenza reciproca più rapida e reattiva basata sulla fiducia internazionale. L'articolo 80dbis dell'AIMP (assistenza reciproca dinamica) consente, in via eccezionale, la trasmissione anticipata di informazioni o prove (a) quando le indagini estere sulla criminalità organizzata o sul terrorismo sarebbero eccessivamente difficili senza questa misura di assistenza reciproca, in particolare a causa del rischio di collusione o perché deve essere preservata la riservatezza del procedimento, oppure (b) per prevenire un pericolo grave e imminente, in particolare la commissione di un atto terroristico. Lo scopo di questa disposizione è quello di consentire una prevenzione efficace in casi urgenti e fondati (ad esempio, presa di ostaggi o attacco terroristico), evitando una reazione troppo tardiva ad atti criminali pianificati, essendo la riservatezza di grande importanza in questo contesto. Da un punto di vista materiale, a differenza dell'art. 18b AIMP, che limita la 18

trasmissione anticipata ai soli dati relativi al traffico informatico, o anche ai dati secondari relativi alle telecomunicazioni tradizionali, l'art. 80dbis AIMP prevede che qualsiasi tipo di prova o informazione possa essere trasmessa anticipatamente in questo modo. Da un punto di vista formale, l'art. 80dbis par. 4 AIMP impone all'autorità di esecuzione di ottenere alcuni impegni aggiuntivi dall'autorità richiedente prima di qualsiasi trasmissione anticipata, in particolare di utilizzare le informazioni o i mezzi di prova solo a fini investigativi e in nessun caso per richiedere, giustificare o pronunciare una decisione definitiva (lettera a) e di rimuovere le informazioni o i mezzi di prova forniti in anticipo dal fascicolo del procedimento straniero se l'assistenza reciproca viene rifiutata (lettera c). Se tutte queste condizioni sono soddisfatte, nulla impedisce la trasmissione anticipata di dati sul contenuto per mezzo e alle condizioni dell'articolo 80dbis dell'IMA.

- 19 Inoltre, la trasmissione anticipata di dati relativi al contenuto può avvenire nell'ambito e secondo le regole di una squadra investigativa comune (SIC; artt. 80dter-80dduodecies AIMP). In questo caso, essa può intervenire anche se non sono soddisfatte le condizioni di cui all'art. 80dbis par. 1 lett. a e b o par. 2 AIMP.

2. Distinzione tra ordine di deposito (art. 265 del Codice di procedura penale) e misura di sorveglianza (art. 269 e segg. del Codice di procedura penale), in particolare per quanto riguarda le caselle e-mail

- 20 La segretezza delle telecomunicazioni è una garanzia costituzionale sancita dall'art. 13 cpv. 1 Cost. Questo diritto è un aspetto essenziale del diritto alla privacy. La sorveglianza della corrispondenza e dei rapporti postali e di telecomunicazione costituisce una grave violazione di questo diritto fondamentale. È quindi fondamentale distinguere tra ciò che è coperto da questa garanzia e ciò che non lo è. A questo proposito, tradizionalmente si applicano due criteri per distinguere i casi in cui le informazioni possono essere ottenute direttamente con un ordine di produzione da quelli in cui è necessaria una richiesta di LSCPT:

- il primo criterio decisivo è il rapporto con la corrispondenza di telecomunicazione;

- il secondo criterio è se i dati richiesti rientrano nell'ambito del diritto fondamentale alla segretezza delle telecomunicazioni tutelato dall'art. 13 cpv. 1 Cost.

Se entrambi i criteri sono soddisfatti, la LSCPT deve essere applicata.

21

In pratica, la maggior parte dei casi riguarderà l'accesso al contenuto delle caselle di posta elettronica (e-mail). Per distinguere tra i dati coperti dal segreto delle telecomunicazioni e quelli che possono essere ottenuti direttamente dalle autorità penali (ordine di archiviazione ai sensi dell'articolo 265 del Codice di procedura penale), il Tribunale federale ha stabilito il criterio dell'ora dell'ultimo accesso (connessione, log) del destinatario dell'e-mail alla sua casella di posta elettronica. Il Tribunale federale ha stabilito che la procedura di comunicazione deve essere considerata conclusa quando il destinatario diventa l'unico proprietario dei dati, ossia quando accede alla sua casella di posta elettronica, indipendentemente dal fatto che abbia effettivamente aperto e letto le e-mail ricevute. In pratica, ciò significa che il pubblico ministero potrà ottenere il contenuto delle e-mail precedenti all'ultima connessione direttamente dal fornitore del servizio (art. 265 CPP), mentre dovrà passare attraverso l'SCPT e il Tribunale per i provvedimenti coercitivi per ottenere il contenuto delle e-mail successive all'ultimo log (art. 269 e seguenti CPP). In altre parole, è l'art. 31 CPC (assistenza reciproca in materia di accesso ai dati memorizzati) e non l'art. 34 CPC che si applica alla raccolta e alla trasmissione di e-mail precedenti all'ultimo log.

22

3. Uso di una falsa identità

A nostro avviso, una persona che, per commettere un reato, utilizza un account su una piattaforma (applicazione di messaggistica, casella di posta elettronica, ecc.) che garantisce un elevato grado di riservatezza (crittografia end-to-end, talvolta abbinata a una crittografia ad accesso zero, pochi o nessun dato richiesto per la registrazione, ecc. Infatti, in assenza di un'identificazione iniziale, ci sono pochi strumenti per verificare che la persona che rivendica questo status sia effettivamente l'utilizzatore della risorsa.

23

Gli autori hanno scritto questo contributo a titolo personale. Le valutazioni e le opinioni presentate sono proprie e non vincolano il Ministero pubblico della Confederazione.

BIBLIOGRAFIA

Aeppli Michael, commentaire de l'art. 18a EIMP, in : Niggli Marcel Alexander/Heimgartner Stefan (édit.), *Basler Kommentar Internationales Strafrecht*, 1^{ère} édition, Bâle 2015.

Dangubic Miro/Clerc Yves, Art. 80d^{bis} IRSG – ein Überblick, *forumpoenale* 4 (2022) p. 287-292.

Ludwiczak Glassey Maria/Bonzanigo Francesca, L'artificielle distinction entre « informations » et « moyens de preuve » en entraide pénale internationale, *Revue Pénale Suisse* 140 (2022) p. 402-427.

Ludwiczak Maria, L'entraide pénale internationale 'dynamique' en bref. Le projet, les débats, le compromis, *Pratique juridique actuelle*, 1 (2021) p. 71–75.

Zimmermann Robert, *La coopération judiciaire internationale en matière pénale*, 5^e édition, Berne 2019.

Donatsch Andreas/Heimgartner Stefan/Meyer Frank/Simonek Madeleine, *Internationale Rechtshilfe*, 2e édition., Zurich et al. 2015.

I MATERIALI

Message concernant la loi fédérale sur la surveillance de la correspondance par poste et télécommunication (LSCPT) du 27 février 2013, FF 2013 2379, consultable sous <https://www.fedlex.admin.ch/filestore/fedlex.data.admin.ch/eli/fga/2013/512/fr/pdf-a/fedlex-data-admin-ch-eli-fga-2013-512-fr-pdf-a.pdf>, consulté en janvier 2024 (cité : Message LSCPT).

Message relatif à l'approbation et à la mise en œuvre de la Convention du Conseil de l'Europe sur la cybercriminalité du 18 juin 2010, FF 2010 4275, consultable sous <https://www.fedlex.admin.ch/filestore/fedlex.data.admin.ch/eli/fga/2010/813/fr/pdf-a/fedlex-data-admin-ch-eli-fga-2010-813-fr-pdf-a.pdf>, consulté en janvier 2024 (cité : Message CCC).

Message relatif à l'arrêté fédéral portant approbation et mise en œuvre de la Convention du Conseil de l'Europe pour la prévention du terrorisme et de son Protocole additionnel et concernant le renforcement des normes pénales contre le terrorisme et le crime organisé, FF 2018 6469 ss, consultable sous

<https://www.fedlex.admin.ch/eli/fga/2018/2301/fr>, consulté en janvier 2024 (cité : Message terrorisme).

Rapport explicatif de la Convention sur la cybercriminalité du 23 novembre 2001, Conseil de l'Europe, Série des traités européens – no 185, consultable sous <https://rm.coe.int/16800ccea4>, consulté en janvier 2024 (cité : Rapport explicatif du Conseil de l'Europe).

Rapport explicatif relatif à la révision totale de l'ordonnance sur la surveillance de la correspondance par poste et télécommunication (OSCPT; RS 780.11) du Service Surveillance de la correspondance par poste et télécommunication, consultable sous https://www.li.admin.ch/sites/default/files/2018-02/Rapport_explicatif_OSCPT.pdf, consulté en janvier 2024 (cité : Rapport explicatif OSCPT).

Recommandation n° R (85) 10 du Comité des Ministres aux États membres concernant l'application pratique de la convention européenne d'entraide judiciaire en matière pénale relative aux commissions rogatoires pour la surveillance des télécommunications du 28 juin 1985, consultable sous : <https://rm.coe.int/09000016804e3071>, consulté en janvier 2024 (cité : Recommandation no R (85) 10).