dossier

XIX legislatura

LE INTERCETTAZIONI: PROFILI DI DIRITTO COMPARATO

aprile 2023
n. 60

servizio studi del Senato

ufficio ricerche sulle questioni istituzionali, giustizia e cultura

SERVIZIO STUDI
Ufficio ricerche sulle questioni istituzionali,
giustizia e cultura
TEL. 066706-2451
studi1@senato.it

XIX legislatura

LE INTERCETTAZIONI: PROFILI DI DIRITTO COMPARATO

aprile 2023
n. 60

a cura di: *Carmen Andreuccioli*
hanno collaborato: *Michela Mercuri, Vladimiro Satta e Federica Faramondi*

Classificazione Teseo: Codice e codificazioni. Diritto comparato. Indagini giudiziarie. Intercettazioni telefoniche. Stati esteri.

I N D I C E

SCHEDE DI LETTURA

Francia

Il quadro normativo

Il segreto della corrispondenza emessa attraverso le comunicazioni elettroniche è garantito dalla legge; le **intercettazioni** sono pertanto misure a **carattere eccezionale** che derogano al principio della segretezza, in un quadro giuridico definito dal Codice di procedura penale (*Code de procédure pénale*), dal Codice della sicurezza interna (*Code de la sécurité intérieure*) e dal Codice della giustizia amministrativa (*Code de la justice administrative*), che ne consentono il ricorso da parte della pubblica autorità solo per tutelare un interesse pubblico.

L'ordinamento ammette **due tipi** di intercettazioni: **giudiziarie** (*Écoutes judiciaires*) e **amministrative o di sicurezza** (*Écoutes administratives*) (*cfr.* la seguente scheda).

Per comunicazioni elettroniche, ai sensi dell'articolo L32 (1°) del Codice delle poste e delle comunicazioni elettroniche (*Code des postes et des communications électroniques*), si intendono tutte le 'emissioni, trasmissioni o le ricezioni di segni, segnali, scritte, immagini o suoni emessi via cavo, via radio, con mezzi ottici o con altri mezzi elettromagnetici'.

Le intercettazioni giudiziarie

Le intercettazioni di conversazioni telefoniche, in ambito giudiziario, pur ampiamente effettuate, fino ad anni recenti non hanno avuto in Francia una regolamentazione specifica, trovando fondamento legale unicamente nella previsione generale dell'articolo 81 del Codice di procedura penale relativo ai poteri del giudice istruttore. Tale situazione ha dato luogo ad abusi che hanno portato alla condanna della Francia da parte della Corte europea dei diritti dell'uomo. In seguito alla pronuncia della Corte, il legislatore ha disciplinato la materia con la legge n. 91-646 del 10 luglio 1991, che ha in più punti novellato il codice di procedura penale, peraltro inserendovi gli articoli da 100-1 a 100-4, 100-6 e 100-7. Tale legge, più volte modificata a partire dal 2004, è stata infine abrogata con *Ordonnance n° 2012-351* del 12 marzo 2012.

Attualmente le intercettazioni giudiziarie sono disciplinate dagli **articoli da 100 a 100-8 c.p.p**.

L'articolo 100, come da ultimo modificato nel 2021 dalla *Loi n° 2021-1729 du 22 décembre 2021 pour la confiance dans l'institution judiciaire*, definisce il quadro giuridico in base al quale possono essere disposte le intercettazioni di corrispondenza effettuate tramite le vie di telecomunicazione. Il potere di ordinare tali mezzi investigativi è attribuito esclusivamente al **giudice istruttore** sotto la sua autorità ed il suo controllo. Il legislatore ha distinto chiaramente le intercettazioni da altri atti che il giudice può disporre senza restrizioni, dettando

condizioni assai rigide. Infatti è possibile ricorrervi solo in materia di **crimini o delitti** per i quali sia prevista una **pena detentiva non inferiore a tre anni** e quando siano ritenute necessarie allo svolgimento delle indagini.

La decisione, che deve essere espressa per iscritto, non ha natura giurisdizionale, di conseguenza non deve essere motivata e **non è suscettibile di ricorso**. La disposizione può concernere l'intercettazione, la registrazione e la trascrizione della corrispondenza inviata tramite strumenti elettronici.

In caso di reato punibile con la reclusione commesso tramite comunicazioni elettroniche sulla linea della vittima, l'intercettazione può ugualmente essere autorizzata, secondo la medesima procedura, se viene effettuata su tale linea su richiesta della vittima.

Le comunicazioni dei legali hanno un livello di riservatezza rafforzato. **Non possono essere effettuate intercettazioni su una linea dipendente dallo studio o dal domicilio di un avvocato**, a meno che non vi siano motivi plausibili per sospettare che questi abbia commesso in tutto o in parte il reato oggetto del procedimento o un reato connesso e a condizione che la misura sia proporzionata alla natura e alla gravità dei fatti. La decisione è adottata con ordinanza, ma essa, proprio per il soggetto coinvolto, deve essere motivata del giudice della libertà e della custodia (*juge des libertés et de la détention*), e richiamata a tal fine da un'ordinanza motivata del giudice istruttore, presa dopo aver consultato il Procuratore della Repubblica.

La decisione, adottata ai sensi dell'articolo 100, deve essere motivata con riferimento alle ragioni di fatto e di diritto che giustificano la necessità di tali operazioni; deve poi contenere tutti gli elementi di identificazione del collegamento da intercettare, il reato per cui si chiede la misura e la sua durata (art. 100-1).

L’art. 100-2 (novellato con legge del 2016) stabilisce che la **durata non può essere superiore a quattro mesi** e che la decisione è rinnovabile alle stesse condizioni di forma e di tempo, senza che la durata complessiva dell'intercettazione possa superare un anno o due anni nel caso dei reati di cui agli articoli 706-73 e 706-73-1 c.p.p.. Ciò al fine di evitare che la misura possa prolungarsi a tempo indeterminato sulla base della decisione iniziale, senza che il giudice ne controlli regolarmente i risultati e ne apprezzi l’utilità.

I due articoli del codice di rito per i quali il tempo massimo per le intercettazioni è raddoppiato disciplinano la procedura applicabile ai reati compiuti dalla criminalità organizzata (omicidio commesso in associazione organizzata, tortura e atti di barbarie compiuti in associazione, stupro, sequestro, tratta di esseri umani, traffico di stupefacenti, terrorismo, riciclaggio, associazione a delinquere, ecc.).

Ai sensi dell’articolo 100-3 c.p.p. (novellato con legge del 2023), ai fini dell'installazione di un dispositivo di intercettazione, il giudice istruttore (o l’ufficiale di polizia giudiziaria da lui incaricato o, sotto il controllo di quest'ultimo, l'agente di polizia giudiziaria) **può richiedere la collaborazione di un operatore qualificato** dipendente da un servizio o da un organismo posto sotto l'autorità o la vigilanza del Ministro competente per le comunicazioni elettroniche, ovvero di

qualsiasi agente qualificato di un operatore di rete o di un fornitore di servizi di comunicazione elettronica autorizzato.

L'articolo 100-4, novellato con medesima legge nel 2023, precisa le formalità relative alle operazioni di intercettazione e registrazione della corrispondenza, per ciascuna delle quali deve essere redatto un processo verbale che indichi la data e l'ora in cui è iniziata e terminata l'operazione. Le registrazioni devono poi essere sigillate.

Ai sensi dell'articolo 100-5 (anch'esso modificato nel 2023), la trascrizione delle registrazioni è limitata alle parti della corrispondenza utili all'accertamento della verità e spetta al giudice istruttore o all'ufficiale di polizia giudiziaria da lui incaricato, ovvero all'agente di polizia giudiziaria o all'assistente investigativo che agisce sotto la sua supervisione, con l'eventuale assistenza di un interprete, qualora le conversazioni siano in lingua straniera. Il verbale deve poi essere inserito nel fascicolo. A pena di nullità, è vietata la trascrizione della corrispondenza con un avvocato relativa all'esercizio dei diritti della difesa e coperta dal segreto professionale, nonché della corrispondenza con un giornalista che consenta l'identificazione di una fonte in violazione dell'articolo 2 della Legge 29 luglio 1881 sulla libertà di stampa.

La conservazione delle registrazioni è consentita fino a quando sia giustificata da necessità di ordine pubblico. L'articolo 100-6 prevede infatti che le registrazioni siano distrutte, su ordine del Procuratore della Repubblica o del Procuratore generale, alla scadenza del termine di prescrizione dell'azione penale pubblica. Dell'operazione di distruzione viene redatto processo verbale.

L'articolo 100-7 pone ulteriori **limiti soggettivi per il ricorso alle intercettazioni**: in primo luogo si esclude la possibilità di registrare le conversazioni sulla linea di un parlamentare se il giudice istruttore non abbia preventivamente informato il Presidente dell'Assemblea di appartenenza. Tali limiti si applicano anche ai magistrati, per i quali è richiesto che ne sia informato il presidente o il procuratore generale della giurisdizione di appartenenza.

Ispirandosi alle disposizioni dell'articolo 56-1 c.p.p. relative alle formalità applicabili in caso di perquisizione di uno studio di avvocato, l'articolo 100-7 c.p.p. precisa inoltre che il giudice istruttore deve informare il Presidente del Consiglio dell'Ordine qualora ritenga necessario disporre l'intercettazione della linea telefonica di un avvocato, ciò nel rispetto della regola della libertà di comunicazione tra l'inquisito e il suo difensore1.

Infine l'articolo 100-8 c.p.p., introdotto con *Ordonnance n° 2016-1636 relative à la décision d'enquête européenne en matière pénale*, dispone che - per l'intercettazione effettuata al di fuori di un ordine di indagine europeo e riguardante un indirizzo di comunicazione elettronica utilizzato nel territorio di uno Stato membro dell'Ue - il giudice istruttore o l'ufficiale di polizia giudiziaria incaricato,

[1] Occorre ricordare che secondo la giurisprudenza d'oltralpe la tutela delle informazioni scambiate tra cliente e proprio difensore di fiducia non è estesa a ogni attività telefonica del difensore in quanto tale, in virtù della sua sola qualifica, ma è circoscritta alle conversazioni attinenti all'attività professionale, concernenti ossia le funzioni del suo incarico professionale di difesa (Cfr. Cour de cassation, criminelle 22 mars 2016, 15-83.205)

notifichi l'intercettazione alla competente autorità di tale Stato, se la persona intercettata si trova nel relativo territorio. La comunicazione avviene prima di disporre l'intercettazione (laddove dal fascicolo emerga che il soggetto si trovi o troverà in quel territorio), ovvero durante l'intercettazione o successivamente ad essa, non appena accertata la presenza del soggetto nello Stato al momento dell'ascolto. Su richiesta dell'autorità competente dello Stato membro, presentata entro 96 ore dal ricevimento della notifica e giustificata dal fatto che l'intercettazione non sarebbe stata autorizzata in analoga procedura nazionale ai sensi della legislazione del medesimo Stato, l'intercettazione non può essere effettuata o deve essere interrotta, ovvero i dati intercettati sul territorio non possono essere utilizzati, dovendo essere rimossi dal fascicolo, ovvero essere utilizzati alle condizioni e per i motivi specificati da tale autorità. Predetta notifica è necessaria, pena invalidità del procedimento, ove si dimostri che l'intercettazione non avrebbe potuto essere autorizzata nell'ambito di analogo procedimento nazionale.

L'uso del **captatore informatico** è stato introdotto nel 2011 con *La loi d'orientation et de programmation pour la performance de la sécurité intérieure* (n. 267 del 14 marzo 2011), codificata negli articoli 706-102-1 e segg. c.p.p. (*De la captation des données informatiques (Articles 706-102-1 à 706-102-5).* In particolare, l'art. 706-102-1 prevede la possibilità di ricorrere alla messa in opera di un dispositivo tecnico il cui scopo, senza il consenso degli interessati, è quello di accedere, ovunque, a dati informatici, registrarli, conservarli e trasmetterli, tal quali sono memorizzati in un sistema informatico, tal quali sono visualizzati su uno schermo per l'utente di un sistema di elaborazione dati automatizzato, tal quali sono inseriti da quest'ultimo mediante la digitazione di caratteri o così come sono ricevuti e trasmessi da periferiche. Al fine di compiere le operazioni tecniche necessarie alla realizzazione di tale dispositivo tecnico, il PM o il giudice istruttore possono designare qualsiasi persona fisica o giuridica autorizzata ed iscritta ad uno degli elenchi di cui all'157 c.p.p. (periti che figurano nell'elenco nazionale redatto dalla Corte di cassazione o in uno degli elenchi redatti dalle corti d'appello alle condizioni di cui alla legge n. 71-498 concernente i periti giudiziari); il PM o il giudice istruttore possono altresì disporre l'impiego di risorse dello Stato sottoposte al segreto della difesa nazionale. Il provvedimento che autorizza l'uso del dispositivo tecnico, a pena di nullità, deve specificare il reato che motiva l'uso di tali operazioni, l'esatta ubicazione o la descrizione dettagliata dei sistemi automatizzati di trattamento dei dati, nonché la durata delle relative operazioni (art. 706-102-3 c.p.p.).

I dati raccolti nell'ambito delle indagini giudiziarie (intercettazioni di conversazioni, dati di connessione, geolocalizzazione, ecc.) sono centralizzati ed elaborati dall'Agenzia nazionale per le tecniche di indagine giudiziaria digitale (*Agence nationale des techniques d'enquêtes numériques judiciaires, Antenj*), istituita nel 2017 con décret n° 2017-614 contestuamente ad un *Comité d'orientation des techniques d'enquêtes numériques judiciaires.* L'Agenzia è un servizio a competenza nazionale facente capo al Guardasigilli e svolge la sua

missione tramite la Piattaforma nazionale per le intercettazioni giudiziarie (*Plateforme nationale des interceptions judiciaires, PNIJ*). Con décret n° 2021-1469 del 9 novembre 2021 l'Agenzia ha sostituito la Delegazione alle intercettazioni giudiziarie (*Délégation aux interceptions judiciaires*)[2] nello svolgimento delle funzioni concernenti le intercettazioni.

La Piattaforma è disciplinata dal codice di procedura penale agli articoli 230-45 e da R40-42 a R40-56 ed è posta sotto la responsabilità del Segretariato generale del Ministero della Giustizia. Quale 'trattamento automatizzato di dati a carattere personalÈ, essa consente l'accesso sicuro ai dati citati esclusivamente agli utenti autorizzati nell'esercizio delle loro funzioni giudiziarie (magistrati, giudici, investigatori, interpreti, agenti doganali, ecc.).

Ai sensi dell'articolo R40-53 c.p.p., come novellato nel 2021 con il citato decreto 2021-1469, la Piattaforma, così come la Agenzia sopra citata, sono poste sotto il controllo di una personalità qualificata in materia, con ruolo di garante, nominata per un periodo non rinnovabile di cinque anni con provvedimento del Guardasigilli, al quale è tenuto ad inviare un rapporto annuale. Nello svolgimento del suo incarico, la personalità è assistita da un comitato di controllo composto da cinque membri. In base all'art. R40-54 c.p.p., i membri del comitato sono individuati come segue:

- un senatore e un deputato scelti rispettivamente dal presidente del Senato, dopo ogni rinnovo parziale del Senato, e dal presidente dell'Assemblea nazionale, per la durata della legislatura, su proposta della commissione competente di ciascuna Assemblea;
- un magistrato della sede onoraria della Corte di cassazione, nominato per un mandato non rinnovabile di cinque anni con provvedimento del Ministro della giustizia;
- una persona qualificata, nominata per un periodo non rinnovabile di cinque anni con provvedimento del Ministro della giustizia, su proposta del Ministro incaricato delle comunicazioni elettroniche;
- una personalità qualificata, nominata per un periodo non rinnovabile di cinque anni con provvedimento del Ministro della giustizia, su proposta del Ministro dell'interno.

Le intercettazioni di sicurezza

Le intercettazioni di sicurezza (c.d. *écoutes administratives*) si distinguono da quelle giudiziarie in quanto destinate a **prevenire la commissione di reati** e non a raccogliere indizi e prove relative a un ipotetico reato già avvenuto.

Sono disposte dal Governo alle condizioni previste dall'ordinamento.

[2] La *Délégation aux interceptions judiciaires*, istituita presso il Ministero della giustizia con decreto n. 2006-1405 del 17 novembre 2006, quale organo sottoposto al Segretario generale del Ministero e diretto da un magistrato, aveva la missione generale di razionalizzare in ambito interministeriale e in termini di procedura, mezzi tecnici e costi, le intercettazioni e la raccolta di dati di traffico disposti dai magistrati, con competenza di carattere tecnico, giuridico e finanziario.

Inizialmente regolata dalla citata legge n. 91-646, ampiamente modificata nel 2004 dalla legge sulle comunicazioni elettroniche e i servizi di comunicazione audiovisiva e infine abrogata nel 2012, la materia è ora disciplinata dal Codice della sicurezza interna (*Code de la sécurité intérieure*), in particolare dagli **articoli da L811-1 a L811-4** e **da L821-1 a L822-4**, contenuti nel Libro VIII del medesimo Codice, dedicato all'*intelligence* (artt. da L801-1 a L 898-1).

Il Codice della sicurezza interna è stato profondamente novellato nel 2015 dalla Legge relativa all'*intelligence* (*LOI n° 2015-912 du 24 juillet 2015 relative au renseignement*), con la quale è stato fornito un quadro giuridico organico per le relative pratiche.

L'articolo L. 801-1 del Codice stabilisce che il rispetto della *privacy* (*la vie privée*), in tutte le sue accezioni, in particolare il segreto della corrispondenza, la tutela dei dati personali e l'inviolabilità del domicilio, è garantito dalla legge. L'autorità pubblica può interferirvi solo in casi di necessità di interesse pubblico previsti dalla legge, nei limiti da essa fissati e nel rispetto del principio di proporzionalità. Di conseguenza, l'autorizzazione e l'attuazione sul territorio nazionale delle tecniche di raccolta di informazioni (di cui ai capitoli da I a III, Titolo V[3], Libro VIII del Codice) possono essere decise solo se:

- provengono da un'autorità giuridicamente competente a farlo;
- risultano conformi a procedimento prestabilito (e indicato nello stesso Titolo);
- rispettano gli obiettivi affidati ai servizi di *intelligence* (di cui all'articolo L. 811-2) o ai servizi designati con decreto del Consiglio di Stato di cui all'articolo L. 811-4 (*cfr. infra*);
- sono giustificate dalle minacce, dai rischi e dalle questioni relative agli interessi fondamentali della Nazione di cui all'articolo L. 811-3;
- le violazioni della *privacy* sono proporzionate a cause e obiettivi.

Il medesimo articolo statuisce che la *Commission nationale de contrôle des techniques de renseignement*, *CNCTR* (**Commissione nazionale per il controllo delle tecniche di *intelligence***), quale autorità amministrativa indipendente, assicuri il rispetto di tali principi e il Consiglio di Stato decida sui ricorsi proposti contro le decisioni relative all'autorizzazione e all'attuazione di tali tecniche e di quelle relative alla conservazione delle informazioni raccolte.

Il ruolo di tale commissione è centrale per gli equilibri del sistema, al punto che le sue riunioni sono quasi quotidiane. Istituita con diversa composizione, nome (CNCIS) e compiti da una legge del 1991, inizialmente essa poteva esercitare solo un controllo *a posteriori*, relativo alla regolarità dell'autorizzazione concessa dal Presidente del Consiglio dei Ministri. Tuttavia, in virtù di una prassi osservata fin dai primi mesi successivi all'entrata in vigore di tale legge e stabilita di comune accordo tra il CNCIS e il Governo, la commissione iniziò a rilasciare pareri anche

[3] *TITRE V: DES TECHNIQUES DE RECUEIL DE RENSEIGNEMENT SOUMISES A AUTORISATION (Articles L851-1 à L855-1 C).*

a priori al Presidente del Consiglio dei Ministri, decidendo poi comunque sulla legittimità e proporzionalità delle richieste di intercettazione.

Attualmente, nell'ambito del quadro sopra delineato, le intercettazioni di sicurezza hanno lo scopo di raccogliere informazioni relative alla **prevenzione** degli attentati alla **sicurezza nazionale**. In particolare, ai sensi dell'art. L811-3 del citato Codice, le finalità che giustificano il ricorso all'utilizzo di tali tecniche sono le seguenti:

- difesa dell'indipendenza nazionale, integrità territoriale e difesa nazionale;
- difesa dei grandi interessi di politica estera, esecuzione degli impegni europei e internazionali della Francia e prevenzione di qualsiasi forma di ingerenza straniera;
- difesa dei grandi interessi economici, industriali e scientifici della Francia;
- prevenzione del terrorismo;
- prevenzione degli attacchi alla forma repubblicana delle istituzioni, delle azioni volte alla ricostituzione o al mantenimento di gruppi disciolti, prevenzione della violenza collettiva di natura tale da turbare gravemente la pace pubblica;
- prevenzione della criminalità e della delinquenza organizzata;
- prevenzione della proliferazione delle armi di distruzione di massa.

In base agli articoli L811-1 e L811-2, introdotti con la legge del 2015, la politica pubblica di *intelligence*, che rientra nella giurisdizione esclusiva dello Stato, contribuisce alla strategia di sicurezza nazionale, nonché alla difesa e alla promozione degli interessi fondamentali della Nazione. I servizi di *intelligence* sono designati con decreto del Consiglio di Stato e le relative missioni, in Francia e all'estero, sono quelle di ricercare, raccogliere, utilizzare e mettere a disposizione del Governo informazioni relative a questioni geopolitiche e strategiche, nonché a minacce e rischi suscettibili di influenzare la vita della Nazione. I servizi contribuiscono alla conoscenza e all'anticipazione di tali eventi, nonché alla prevenzione e al contrasto dei relativi rischi e minacce. I servizi agiscono nel rispetto della legge, sotto l'autorità del Governo e in conformità con le linee guida definite dal *Conseil national du renseignement*, comitato specializzato del *Conseil de défense et de sécurité nationale* (Consiglio nazionale di difesa e sicurezza), incaricato di definire la strategia nazionale di *intelligence*, ovvero gli orientamenti strategici, le priorità in materia di intelligence, la pianificazione delle risorse umane e tecniche per i relativi servizi. È organo di altissimo livello essendo presieduto dal Capo dello Stato e partecipandovi il Primo Ministro, i ministri competenti e i direttori dei servizi di *intelligence* la cui presenza è richiesta dall'ordine del giorno, nonché il Coordinatore nazionale dell'*intelligence* (*Coordonnateur national du renseignement*).

L'articolo L. 811-4, modificato nel 2016, demanda a un **decreto del Consiglio di Stato**, emanato su parere della citata *CNCTR*, la designazione di **servizi diversi da quelli di *intelligence***, facenti comunque capo ai **ministri della difesa, dell'interno e della giustizia nonché ai ministri responsabili per l'economia, il bilancio o le dogane**, che possono essere autorizzati ad utilizzare le tecniche di raccolta di informazione sottoposte ad autorizzazione (di cui al Titolo V, Articoli da L851-1 a L855-1 C) alle condizioni ivi previste. In tale decreto occorre specificare, per ogni servizio, le finalità di cui all'articolo L. 811-3 e le tecniche che possono dar luogo all'autorizzazione.

La **procedura applicabile alle tecniche di raccolta di informazione soggette ad autorizzazione** è disciplinata dal Titolo II Libro VIII del Codice (artt. da L821-1 a L 822-4).

Il **carattere eccezionale di tali intercettazioni** emerge dalla procedura rigorosa prescritta dalle relative disposizioni.

Ai sensi dell'art. L821-1, come novellato con legge del 2021, l'attuazione sul territorio nazionale delle tecniche di raccolta di informazioni è, infatti, subordinata alla **preventiva autorizzazione del Presidente del Consiglio dei Ministri**, rilasciata **previo parere della CNCTR**. Gli agenti che realizzano materialmente l'attività sono designati e autorizzati individualmente.

Laddove l'autorizzazione sia rilasciata dopo parere sfavorevole della CNCTR, il **Consiglio di Stato** è immediatamente **adito dal presidente della CNCTR** o, in mancanza, da uno dei componenti e il provvedimento di autorizzazione del Presidente del Consiglio dei Ministri non può essere eseguito prima della pronuncia del Consiglio di Stato, salvo in caso di urgenza debitamente motivata e se il Presidente del Consiglio dei Ministri ne abbia disposto l'immediata attuazione.

Quando è adito ai sensi dell'articolo in esame, il Consiglio di Stato delibera alle condizioni previste dal Capitolo III-bis, Titolo VII, Libro VII del *Code de justice administrative* (Codice di giustizia amministrativa, articoli da L773-1 a L773-8), che stabilisce una composizione particolare, dacché si deve garantire la segretezza dell'oggetto della questione.

In base all'art. L821-2 (come modificato con legge del 2016) la predetta autorizzazione è rilasciata **su richiesta scritta e motivata** del Ministro della difesa, del Ministro dell'interno, del Ministro della giustizia o dei ministri responsabili dell'economia, del bilancio o delle dogane. Ciascun ministro può delegare tale incarico solo individualmente a collaboratori diretti autorizzati al mantenimento del segreto della difesa nazionale. La richiesta deve specificare: la tecnica o le tecniche da implementare; il servizio per il quale si presenta; lo scopo perseguito; il motivo delle misure; il periodo di validità dell'autorizzazione; le persone/luoghi interessati. In caso di rinnovo di un'autorizzazione, la richiesta deve esporre i motivi per i quali il rinnovo è giustificato in relazione alle finalità perseguite.

L'art. L821-3 prevede che la richiesta sia comunicata al presidente della Commissione nazionale per il controllo delle tecniche di *intelligence* (o, in mancanza, a uno dei membri di cui ai punti 2° e 3° dell'art. L. 831-1, concernente la composizione della Commissione, ovvero membri consiglieri di Stato o magistrati), che esprime parere al Presidente del Consiglio entro ventiquattro ore. Se la richiesta è esaminata dalla formazione ristretta o dalla formazione plenaria della Commissione, il Presidente del Consiglio dei Ministri ne è informato e il parere espresso entro settantadue ore. I pareri sono comunicati tempestivamente al Presidente del Consiglio dei Ministri; in difetto di comunicazione inviata entro i termini previsti, essa si considera data.

In base all'art. L821-4, l'autorizzazione all'intercettazione è rilasciata dal Presidente del Consiglio dei Ministri per un **periodo massimo di quattro mesi** (rinnovabile con medesima procedura, ma senza l'indicazione di un numero massimo di volte); questi può delegare individualmente tale incarico solo a collaboratori diretti autorizzati a mantenere il segreto della difesa nazionale. Quando l'autorizzazione è rilasciata a seguito di parere negativo della CNCTR, deve indicare le ragioni per le quali tale parere è stato disatteso. L'autorizzazione del Presidente del Consiglio è comunicata senza indugio al Ministro incaricato della sua esecuzione nonché alla Commissione; la richiesta e l'autorizzazione sono protocollate dalla Presidenza del Consiglio dei Ministri e i registri sono messi a disposizione della CNCTR.

L'art. L821-7 (come novellato nel 2021) prevede che i parlamentari, i magistrati, gli avvocati e i giornalisti non possano essere sottoposti a raccolta di informazioni, in ragione dell'esercizio del loro mandato o della loro professione. Laddove la richiesta di autorizzazione riguardi tali categorie di persone, ai fini dell'espressione del relativo parere, è necessario l'esame in seduta plenaria dalla CNCTR e non può essere invocata l'urgenza prevista dal citato art. L. 821-1. La Commissione è informata delle modalità di svolgimento delle autorizzazioni rilasciate ai sensi dell'articolo in commento e le trascrizioni delle informazioni in tal modo raccolte sono trasmesse alla Commissione, la quale accerta il carattere necessario e proporzionato delle eventuali violazioni apportate alle garanzie connesse all'esercizio di tali attività professionali o mandati.

Gli articoli L822-2 e L822-3 disciplinano la durata della conservazione e delle trascrizioni. In linea generale, la registrazione di una conversazione telefonica viene distrutta entro e non oltre **30 giorni** dalla raccolta delle informazioni, salvo eccezioni; vengono trascritte solo le informazioni sulla sicurezza nazionale e la trascrizione deve essere distrutta non appena la sua conservazione non sia più indispensabile.

Il Codice della sicurezza interna disciplina la *Commission nationale de contrôle des techniques de renseignement*, *CNCTR* (**Commissione nazionale per il controllo delle tecniche di *intelligence***) agli articoli da L831-1 a L833-11.

Istituita con la citata Legge 24 luglio 2015 relativa all'*intelligence*, la Commissione è stata successivamente inquadrata dalla Legge n° 2017-55 del 20 gennaio 2017 sullo statuto generale delle autorità amministrative indipendenti e delle autorità pubbliche indipendenti.
La CNCTR ha dunque il compito di garantire che le tecniche di *intelligence* siano applicate legalmente sul territorio nazionale, svolgendo controlli preventivi e successivi. A tal fine, come sopra già ricordato, salvo casi di assoluta urgenza, esprime un parere su ogni richiesta di utilizzo di una tecnica prima che il Primo Ministro assuma una decisione (controllo *a priori*) e verifica l'esecuzione delle autorizzazioni accordate dal Primo Ministro (controllo *a posteriori*), potendo peraltro deliberare su qualsiasi argomento di sua competenza, sia di propria iniziativa che su richiesta del Primo Ministro o del Parlamento.
La CNCTR ha sostituito la precedente **Commissione nazionale di controllo delle intercettazioni di sicurezza** (*Commission nationale de contrôle des interceptions de sécurité, CNCIS*), che era stata istituita con la legge del 1991 quale organo di garanzia contro eventuali abusi del potere esecutivo, ma che prevedeva solo un controllo *a posteriori* (si veda qui una scheda di riepilogo).

La composizione e l'organizzazione della CNCTR sono indicate agli articoli L831-1 e L831-2 del Codice della sicurezza interna. In base all'art. L831-1, novellato nel 2017, essa si configura quale autorità amministrativa indipendente composta da nove membri, così ripartiti:

1: quattro parlamentari (due deputati e due senatori), nominati in modo da assicurare la rappresentanza pluralistica del Parlamento;

2: due membri del Consiglio di Stato, di grado almeno pari a quello di Consigliere di Stato, nominati dal Vicepresidente del Consiglio di Stato;

3: due magistrati della Corte di Cassazione, nominati congiuntamente dal primo presidente e dal pubblico ministero della Cassazione;

4: una personalità qualificata in virtù della sua conoscenza delle comunicazioni elettroniche, nominata su proposta del Presidente dell'*Autorité de régulation des communications électroniques, des postes et de la distribution de la presse, ARCEP*.

Le procedure di designazione o nomina dei membri di cui ai punti 1-3 devono **assicurare pari rappresentanza di genere**.

Il presidente della Commissione è nominato con decreto del Presidente della Repubblica tra i membri di cui ai punti 2 e 3. Il mandato dei membri, ad eccezione dei parlamentari (per i quali vale la regola di durata del mandato elettivo), è di sei anni, non rinnovabile. I membri del Consiglio di Stato o della Corte di Cassazione si rinnovano per metà ogni tre anni. La Commissione può riunirsi in due formazioni collegiali, entrambe presiedute dal Presidente della Commissione: la plenaria, comprendente tutti i membri sopra menzionati, e la

formazione ristretta, composta dai membri di cui ai punti 2-4 (i due membri del Consiglio di Stato, i due magistrati di Cassazione e la personalità qualificata). La formazione ristretta e la formazione plenaria possono validamente deliberare solo se, rispettivamente, sono presenti almeno tre o quattro membri.

L'articolo L. 832-2 del Codice di sicurezza interna disciplina il regime delle incompatibilità, vietando ai membri della Commissione di avere interessi diretti o indiretti nei servizi di *intelligence* o negli operatori di comunicazioni elettroniche o nei fornitori di servizi Internet, nonché prevedendo l'incompatibilità del mandato con qualsivoglia attività professionale o altro impiego pubblico esercitati a tempo pieno, nonché con la titolarità di qualunque incarico elettivo, ad eccezione dei membri parlamentari.
Ai sensi dell'art. L. 832-5, i lavori della Commissione sono coperti dal segreto della difesa nazionale: ciò comporta il rispetto di specifiche misure di sicurezza, derivanti dagli artt. 413-9 e segg. c.p. I membri della Commissione sono autorizzati *ex lege* all'accesso alle informazioni classificate rilevanti per lo svolgimento delle loro funzioni, mentre gli agenti della Commissione sono soggetti a specifica procedura di abilitazione.
La Commissione svolge i propri lavori in base ad un regolamento interno, adottato con delibera 2/2017 del 23 marzo 2017.

Germania

Le intercettazioni a fini di giustizia

Le intercettazioni a fini di giustizia sono disciplinate dal Codice di procedura penale (*Strafprozessordnung, StPO*)[4], che distingue tra la sorveglianza acustica all'interno (art. 100c StPO) e all'esterno (art. 100f StPO) di locali privati e la sorveglianza delle telecomunicazioni (art. 100a StPO).

La sorveglianza delle telecomunicazioni e la sorveglianza acustica al di fuori dei locali privati possono essere ordinate solo se si sospetta un reato grave (artt. 100a (1) frase 1, n. 1, (2), 100f (1) StPO). La sorveglianza di locali privati richiede anche il sospetto di un reato particolarmente grave (art. 100c (1) n. 1 StPO). Tutte le misure sono soggette al requisito che possono essere ordinate solo come misura secondaria se altri mezzi per accertare i fatti o determinare il luogo in cui si trova l'imputato o il luogo in cui si trova un co-accusato non offrirebbero altrimenti alcuna prospettiva di successo o sarebbero molto più difficili (art. 100a (1) frase 1, n. 1, 100c (1) n. 4, 100f (1) StPO). Inoltre, la sorveglianza acustica di locali privati può essere ordinata solo se si può presumere che la sorveglianza porterà effettivamente alla registrazione delle dichiarazioni dell'imputato (art. 100c (1) n. 3 StPO). Infine, tutti gli atti di indagine descritti sono inammissibili se vi sono indicazioni che vengono utilizzati esclusivamente per ottenere informazioni sulla vita privata (art. 100d (1) StPO, art. 100f (4) StPO in combinato disposto con l'art. 100d (1) StPO).

L'art. 100d (1) dispone che se vi sono effettive indicazioni per presumere che una misura ai sensi delle Sezioni da 100a a 100c fornisca solo conoscenze relative alla sfera della vita privata, la misura è inammissibile.

In base al diritto processuale, la sorveglianza delle telecomunicazioni e la sorveglianza acustica al di fuori dei locali privati devono, come principio generale, essere ordinate da un tribunale. In circostanze eccezionali, l'ordine può essere impartito anche dalla Procura della Repubblica, ma tale ordine richiede l'autorizzazione del tribunale entro tre giorni lavorativi (art. 100e (1) frasi 1 e 2 StPO, art. 100f (4) StPO, in combinato disposto con l'art. 100e (1) frasi 1 e 2 StPO). Per contro, la sorveglianza acustica di locali privati richiede sempre un'ordinanza del tribunale (art. 100e (2) frase 1 StPO). L'ordine per la sorveglianza delle telecomunicazioni e la sorveglianza acustica al di fuori di locali privati deve essere generalmente limitato a un massimo di tre mesi e non può essere prorogato per più di tre mesi per un totale massimo di sei mesi (art. 100e (1) frasi 4 e 5 StPO, art. 100f (4) StPO, in combinato disposto con l'art. 100e (1) frasi 4 e 5 StPO). La sorveglianza acustica di locali privati, invece, deve essere generalmente limitata a un periodo di un mese e non può essere prorogata per più di un mese (art. 100e (2)

[4] Traduzione in inglese disponibile alla seguente URL: https://www.gesetze-im-internet.de/englisch_stpo/index.html.

frasi 4 e 5, 100f (4) StPO). Tutte le misure sono soggette al requisito che i dati ottenuti attraverso la sorveglianza devono essere cancellati immediatamente se non sono più necessari ai fini dell'esercizio dell'azione penale o di un eventuale riesame delle misure da parte del tribunale (art. 101(8) StPO). Le persone interessate devono essere informate una volta terminata la misura investigativa (art. 101 (4) frase 1 n. 3, 5, 6 StPO).

Le autorità penali sono soggette all'obbligo di tenere fascicoli separati ("fascicoli speciali") per la sorveglianza acustica di locali privati e per la sorveglianza al di fuori di tali locali ai sensi dell'articolo 101 (2) StPO (cfr. anche articolo 68 (4) frasi 3 e 4 StPO). I materiali conservati negli archivi speciali e i supporti di dati utilizzati per la conservazione possono essere ispezionati dopo la loro divulgazione dalle persone interessate e dai loro avvocati difensori secondo i principi generali dell'accesso agli archivi (art. 147 StPO). Lo stesso vale per i dati ottenuti nell'ambito della sorveglianza delle telecomunicazioni.

I dati ottenuti attraverso la sorveglianza delle telecomunicazioni o la sorveglianza acustica al di fuori dei locali privati possono essere utilizzati solo in altri procedimenti penali per indagare su reati che, considerati singolarmente, avrebbero potuto giustificare l'ordine di tale misura (art. 479 (2) frase 1 StPO, in combinato disposto con l'art. 161 (3) StPO). I dati ottenuti attraverso una misura di sorveglianza possono essere utilizzati anche da altre autorità, senza il consenso della persona interessata, solo nel caso in cui la misura è necessaria per scongiurare un pericolo per la vita, l'incolumità fisica o la libertà di una persona o per la sicurezza o l'esistenza della Federazione o di uno Stato (art. 479 (2) frase 2 n. 2 StPO).

I dati ottenuti attraverso la sorveglianza acustica di locali privati possono essere utilizzati solo in altri procedimenti penali per indagare su reati che avrebbero potuto di per sé giustificare l'ordine di tale misura (art. 100e (6) n. 1 StPO). L'accesso a questi dati è consentito solo per scongiurare un pericolo in caso di pericolo di morte o di pericolo imminente, ad esempio per la salute, la sicurezza dello Stato o oggetti di grande valore (art. 100e (6) n. 2 StPO).

Le misure ordinate ai sensi degli artt. 100a, c, f StPO sono eseguite dall'autorità di polizia investigativa nell'ambito di un procedimento investigativo. Gli artt. 100c (1), 100f (1) StPO consentono l'intercettazione e la registrazione di discorsi privati con "mezzi tecnici". Il legislatore non ha deliberatamente definito l'elenco degli strumenti tecnici utilizzabili ai fini delle intercettazioni, al fine di dare la possibilità, alle autorità procedenti, di utilizzare la tecnologia ritenuta più adatta per la misura specifica, in accordo con gli sviluppi tecnologici. Tuttavia, i mezzi tecnici possono essere utilizzati solo per registrare il parlato: non è consentito utilizzare i mezzi tecnici in locali privati per scattare fotografie o effettuare registrazioni video. Oltre all'uso effettivo dei "mezzi tecnici", la legge autorizza anche le misure di accompagnamento che esso richiede, come ad esempio l'ingresso segreto ripetuto nei locali privati allo scopo di installare o rimuovere gli strumenti tecnologici utilizzati per l'applicazione della misura di controllo. Per quanto riguarda la sorveglianza delle telecomunicazioni, che oggi avviene per lo

più in forma criptata su Internet, l'art. 100a (1) frase 2 StPO permette alle autorità di polizia di monitorare e registrare le comunicazioni effettuate in forma criptata dalla persona interessata e dai suoi partner di comunicazione (ancora) in forma non criptata con l'ausilio di un *software* di sorveglianza, che deve soddisfare i requisiti di cui all'art. 100a (5) frase 1, n. 1, lett. a StPO. L'art. 100a (1) frase 2 StPO consente contemporaneamente l'installazione di *software* di de-crittografia e trasmissione sul computer sottoposto a sorveglianza come misura supplementare.

La disciplina delle intercettazioni preventive

La sorveglianza segreta delle telecomunicazioni e l'acquisizione da remoto di dati digitali possono essere utilizzati anche a scopo preventivo; tuttavia, la sorveglianza delle telecomunicazioni è più estesa delle perquisizioni a distanza.

La base giuridica per autorizzare la sorveglianza delle telecomunicazioni si trova in tutte le leggi di polizia dei *Länder*, nonché nella Legge sull'Ufficio federale di polizia criminale e sulla cooperazione tra il governo federale e quello statale in materia penale (*Bundeskriminalamtgesetz, BKAG*). Anche i servizi segreti federali, l'Ufficio federale per la protezione della Costituzione (*Bundesamt für Verfassungsschutz*), l'Ufficio federale di controspionaggio militare (*Bundesamt für den Militärischen Abschirmdienst*) e il Servizio federale di intelligence (*Bundesnachrichtendienst*), possono utilizzare lo strumento della sorveglianza delle telecomunicazioni a determinate condizioni, ai sensi della Legge per la limitazione della privacy di lettere, poste e telecomunicazioni (*Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses*, *Artikel10-Gesetz*, *G10*). Anche gli Uffici statali per la protezione della Costituzione (*Landesämter für Verfassungsschutz*) hanno a disposizione basi legali per autorizzare questo strumento.

A livello federale, l'Ufficio federale di polizia criminale (*Bundeskriminalamt, BKA*) e il Servizio federale di *intelligence* possono utilizzare lo strumento della ricerca a distanza; quest'ultimo, tuttavia, solo all'estero e solo in relazione a cittadini stranieri (cfr. art. 34 della Legge sui servizi segreti federali, *Gesetz über den Bundesnachrichtendienst, BND*). L'Ufficio federale per la protezione della Costituzione e il Servizio militare di controspionaggio non dispongono di questo strumento di sorveglianza. In alcuni *Länder*, le autorità di polizia sono autorizzate a utilizzare lo strumento dell'acquisizione da remoto di dati digitali. La sorveglianza delle telecomunicazioni è soggetta a rigorosi requisiti costituzionali derivanti dalla riservatezza della corrispondenza, della posta e delle telecomunicazioni sancita dall'articolo 10 della Costituzione (*Grundgesetz*)[5]. I requisiti per le ricerche a distanza sono ancor più severi in quanto ledono il "diritto fondamentale alla riservatezza e all'integrità dei sistemi informatici", che la Corte

[5] Disponibile in lingua inglese alla seguente URL: https://www.gesetze-im-internet.de/englisch_gg/index.html.

costituzionale federale ha ricavato dal diritto generale della persona di cui all'articolo 2 (1), in combinato disposto con l'articolo 1 (1) Cost.

Le basi legali per l'autorizzazione sono quindi definite in modo rigoroso. Per l'Ufficio federale di polizia criminale (BKA), esse derivano dagli articoli 49 e 51 della citata legge BKAG. Tali articoli stabiliscono che il BKA può effettuare l'acquisizione da remoto di dati digitali, ad esempio, se "vi è una minaccia alla [...] vita, all'incolumità o alla libertà di una persona o [...] a beni pubblici, la cui minaccia pregiudica le fondamenta o l'esistenza della Federazione o di un *Land* o le fondamenta della vita delle persone" (art. 49 (1) n. 1 BKAG). La sorveglianza delle telecomunicazioni è possibile se "è necessaria per scongiurare un pericolo imminente per l'esistenza o la sicurezza della Federazione o di un *Land* e o per la vita, l'incolumità o la libertà di una persona o di oggetti di valore significativo, la cui conservazione è di interesse pubblico" (art. 51 (1) n. 1 BKAG). Sia le perquisizioni a distanza che la sorveglianza delle telecomunicazioni possono essere effettuate solo se autorizzate da un giudice (art. 49 (4), art. 51 (3) BKAG). Una volta terminata la misura, le persone soggette alla sorveglianza devono essere informate (cfr. art. 74 (1) nn. 6, 8 BKAG).

Spagna

Il quadro normativo

Le indagini tecnologiche sono considerate una misura limitativa dei diritti fondamentali, riconosciuti dall'articolo 18 della Costituzione spagnola del 1978.

In particolare, l'articolo 18.3 Cost. stabilisce che "è garantito il segreto delle comunicazioni e, in particolare, di quelle postali, telegrafiche e telefoniche, salvo decisione giudiziaria". Tale articolo era già presente in altre costituzioni storiche spagnole, come quelle del 1869, 1876 e 1931.

Poiché il diritto alla segretezza delle comunicazioni è annoverato tra i diritti fondamentali, perché esso sia limitato non è sufficiente che sia approvata una legge "comune". Si richiede infatti che la disciplina regolatoria sia contenuta in una *Ley Orgánica*, da approvare a maggioranza qualificata.

Una prima attuazione del disposto costituzionale si ebbe nel 1988 con l'introduzione - tramite Legge Organica 4/1988 - di sintetiche disposizioni relative alla possibile limitazione del suddetto diritto, per effetto della novella recata all'articolo 579 del Codice di procedura penale (*Ley de Enjuiciamiento Criminal*, *LECrim*), concernente il fermo della corrispondenza.

In particolare, con la norma del 1988 veniva consentito al giudice di accordare il sequestro della corrispondenza privata, postale e telegrafica di una persona indagata, se vi fossero stati "indizi di ottenere in tali modi la scoperta o la conferma di alcun fatto o circostanza importante del procedimento" (comma 1). Lo stesso poteva avvenire, mediante risoluzione motivata, per l'intercettazione delle comunicazioni telefoniche dell'interessato (comma 2), sempre in presenza dei medesimi indizi. La norma prevedeva inoltre, al comma 3, che le comunicazioni potessero essere tenute sotto osservazione per un periodo di tre mesi, prorogabile per uguali periodi di tempo, sempre mediante risoluzione motivata del giudice, per "le persone per le quali vi siano indizi di responsabilità penale, così come per le comunicazioni delle quali esse si servano per la realizzazione dei loro scopi criminali". Veniva infine disposto, al comma 4, che, in caso di urgenza, quando le indagini si attuassero per l'accertamento di reati collegati all'attività di bande armate o di elementi terroristici, l'adozione della misura di cui al comma 3 potesse essere deliberata dal Ministro dell'Interno o, in sua vece, dal Direttore della Sicurezza dello Stato, comunicando le motivazioni per iscritto al giudice competente, per la conferma o la revoca di tale decisione entro 72 ore.

Il legislatore spagnolo, a differenza di altre normative europee, non specificava dunque i presupposti e i requisiti per l'adozione di una risoluzione giudiziaria valida, né per l'accertamento degli indizi richiesti dalla legge. È quindi stata la giurisprudenza del Tribunale Supremo e del Tribunale Costituzionale a porre alcuni principi fondamentali in materia, a introdurre la definizione stessa di 'intercettazione telefonica', nonché a precisare i concetti espressi dal legislatore (*cfr. infra*).

Nonostante gli sforzi della giurisprudenza e della dottrina per colmare le lacune del novellato articolo 579 c.p.p., la Spagna è stata più volte condannata dalla Corte europea dei diritti dell'uomo per violazione dell'articolo 8 CEDU a fronte della scarsa qualità legislativa del novellato articolo del codice di rito, specie per l'insufficiente tutela dei diritti degli indagati[6].

Negli anni successivi, tanto il Tribunale Supremo quanto il Tribunale Costituzionale hanno tentato di colmare le lacune dell'art. 579 c.p.p., al fine di evitare nuove condanne europee. In diverse sentenze, la giurisprudenza spagnola ha quindi via via individuato i requisiti che devono necessariamente essere soddisfatti per la validità delle intercettazioni:

a) esclusività giurisdizionale, nel senso dell'indispensabilità dell'intervento del giudice per l'intercettazione di comunicazioni;

b) scopo esclusivamente probatorio dell'intercettazione, al fine di determinare l'esistenza del reato e le persone responsabili dello stesso;

c) adozione della misura solo quando non esistono altri mezzi di indagine che possano arrecare pregiudizio minore ai diritti fondamentali della persona interessata;

d) rispetto del principio di proporzionalità della misura e relativa adozione solo in caso di reati gravi e di rilevanza sociale (il nocumento ai diritti fondamentali dell'individuo deve essere sempre compensato da uno scopo più elevato);

e) limitazione nel tempo della misura, che non può mai essere estesa a tempo indeterminato o in modo eccessivo;

f) divieto di utilizzo della misura per un'indagine generale, bensì per l'indagine concernente uno specifico atto criminoso;

g) sufficiente motivazione del provvedimento giudiziario di concessione della misura.

Con la promulgazione della *Ley Orgánica 13/2015*, recante modifica del codice di rito per il rafforzamento delle garanzie processuali e la regolamentazione delle misure di investigazione tecnologica, è stato introdotto un quadro finalmente esaustivo alla materia. La legge organica 13/2015 è costituita da un articolo unico estremamente lungo che modifica, per quanto di interesse nella presente trattazione, le seguenti disposizioni del *Ley de Enjuiciamiento Criminal*[7]:

- la rubrica del Titolo VIII, Libro II, che viene così riformulata: «*Titolo VIII. Le misure di investigazione limitative dei diritti riconosciuti dall'articolo 18 della Costituzione*» (artt. da 545 a 588-*octies*);

- l'art. 579 c.p.p, concernente il sequestro e l'apertura della corrispondenza scritta e telegrafica, che viene novellato al fine di limitarne l'ambito di applicazione materiale e disciplinare i periodi massimi di durata e le eccezioni alla necessità di un'autorizzazione giudiziaria secondo una consolidata dottrina giurisprudenziale. In particolare, la riforma sceglie, a differenza di altri modelli comparati, di non proporre un elenco di reati per i quali si autorizza il ricorso

[6] Si ricorda, ad es. nel 2003 la sentenza Prado Bugallo *vs* Spagna.

[7] Occorre ricordare che il processo penale spagnolo è disciplinato dalla *ley de enjuiciamento criminal*.

alle intercettazioni. A questo sistema**, è preferita una triade di ipotesi alternative per stabilire l'ambito di applicazione di altre misure investigative**. La prima opera come una limitazione generica, di natura quantitativa, legata alla gravità della pena: reati intenzionali puniti con un massimo di oltre tre anni di reclusione. La seconda le permette le intercettazioni quando i reati siano commessi all'interno di un gruppo o di un'organizzazione criminale. La terza ipotesi concerne il terrorismo;

- viene introdotto un nuovo articolo 579-*bis*, al fine di disciplinare l'utilizzo di informazioni ottenute dal sequestro/apertura della corrispondenza scritta e telegrafica come mezzo di indagine o prova in altri procedimenti penali, specie per quanto concerne il trattamento delle cosiddette "scoperte casuali" e la prosecuzione della misura di indagine nel relativo procedimento, per il quale è necessaria una nuova ordinanza del tribunale che convalidi la situazione;

- nel Titolo VIII, Libro II, vengono inseriti i seguenti **nuovi Capitoli:**

    - **Capitolo IV**, recante ***Disposizioni comuni per l'intercettazione di comunicazioni telefoniche e telematiche, l'acquisizione e la registrazione di comunicazioni orali mediante l'uso di dispositivi elettronici, l'uso di dispositivi tecnici per il monitoraggio, la localizzazione e la cattura di immagini, la registrazione di dispositivi di immagazzinamento massivo di informazioni e le registrazioni da remoto su dispositivi informatici***, articoli da 588-*bis-a* (Principi direttivi) a 588-*bis-k* (Distruzione delle registrazioni);
    - **Capitolo V**, recante ***L'intercettazione di comunicazioni telefoniche e telematiche***, articoli da 588-*ter-a* (Presupposti) a 588-*ter-m* (Identificazione di titolari o terminali o dispositivi di connettività);
    - **Capitolo VI**, recante ***Acquisizione e registrazione di comunicazioni orali tramite utilizzo di dispositivi elettronici,*** articoli da 588-*quater-a* (Registrazione di comunicazioni orali dirette) a 588-*quater-e* (Cessazione);
    - **Capitolo VII**, recante ***Utilizzo di dispositivi tecnici per l'acquisizione di immagini, il tracciamento e la localizzazione***, articoli da 588-*quinquies-a* (Acquisizione di immagini in luoghi o spazi pubblici) a 588-*quinquies-c* (Durata della misura);
    - **Capitolo VIII**, recante ***Registrazione di dispositivi di archiviazione massiva di informazioni***, articoli da 588-*sexies-a* (Necessità di una motivazione personalizzata) a 588-*sexies-c* (Autorizzazione giudiziaria);
    - **Capitolo IX**, recante ***Registrazioni da remoto su apparecchiature informatiche***, articoli da 588-*septies-a* a (Presupposti) a 588-*septies-c* (Durata);
    - **Capitolo X**, recante ***Misure di sicurezza***, articolo 588-*octies* (Ordine di conservazione dei dati).

Il legislatore del 2015 ha ritenuto opportuno riversare in una fonte normativa i principi definiti dal Tribunale Costituzionale per determinare la validità dell'atto di ingerenza in diritti costituzionalmente garantiti. Di conseguenza, l'art. 588-*bis-a* c.p.p., nel disciplinare i **principi direttivi**, dispone che qualsivoglia misura di interferenza risponda ai principi di **specialità, adeguatezza, eccezionalità, necessità e proporzionalità**, la sussistenza dei quali deve essere sufficientemente motivata nella decisione di abilitazione, in cui il giudice determinerà la natura e l'estensione della misura in relazione alla ricerca specifica e ai risultati attesi.

Il principio di **specialità** richiede che lo scopo della misura sia quello di far luce su uno specifico atto punibile, vietando misure di indagine tecnologica di natura prospettica (valga per tutte la Sentenza del Tribunale Costituzionale n. 253 dell'11 settembre 2006). Non possono quindi essere autorizzate misure finalizzate a prevenire o scoprire reati o chiarire sospetti senza un fondamento oggettivo.

Il principio di **adeguatezza** serve a definire l'ambito oggettivo e soggettivo e la durata del provvedimento in ragione della sua utilità.

In applicazione dei principi di **eccezionalità e necessità**, la misura può essere disposta: quando non siano disponibili all'indagine, per le loro caratteristiche, altri provvedimenti meno gravosi per i diritti fondamentali dell'indagato o dell'imputato e ugualmente utili per l'accertamento del fatto, ovvero quando la scoperta o l'accertamento del fatto indagato, dell'autore o degli autori, della loro ubicazione o l'individuazione degli effetti del reato sono gravemente ostacolati senza il ricorso a tale misura.

La misura è, infine, considerata **proporzionata** solo quando, tenuto conto di tutte le circostanze del caso, il sacrificio dei diritti e degli interessi lesi non eccede il beneficio derivante dalla relativa adozione all'interesse pubblico e dei terzi.

Per la **ponderazione degli interessi confliggenti**, la valutazione dell'interesse pubblico si baserà sulla **gravità del fatto**, sulla sua **rilevanza sociale** o sull'**ambito tecnologico di produzione**, sull'**intensità degli indizi** esistenti e sulla **rilevanza del risultato** perseguito con la limitazione del diritto.

L'art. 588-*bis-b* disciplina la **richiesta di autorizzazione giudiziale**, stabilendo che il giudice istruttore può disporre l'applicazione delle misure di indagine tecnologica d'ufficio, ovvero su richiesta del PM o della polizia giudiziaria. In tal caso, la richiesta deve contenere:

- la descrizione del fatto oggetto di indagine e l'identità della persona oggetto di indagine o di altro soggetto interessato dalla misura, a condizione che tali informazioni siano note;
- l'esposizione dettagliata delle ragioni che giustificano la necessità del provvedimento, nonché gli indizi di criminalità emersi nella fase di indagine precedente alla richiesta di autorizzazione dell'atto di ingerenza;
- gli estremi identificativi della persona indagata o imputata e, se del caso, i mezzi di comunicazione utilizzati per consentire l'esecuzione della misura;
- l'entità della misura, specificandone il contenuto;
- l'unità investigativa della polizia giudiziaria incaricata dell'intervento;
- la forma di esecuzione della misura;

- la durata della misura richiesta;
- il soggetto obbligato all'esecuzione della misura, se noto.

Ai sensi dell'articolo 588-*bis*-*c* c.p.p., concernente la **decisione giudiziale**, il giudice istruttore autorizza o nega la misura richiesta con ordinanza motivata, sentito il PM, entro il termine massimo di 24 ore dalla presentazione della domanda. Tale termine viene interrotto laddove il giudice chieda la proroga o la precisazione dei termini della richiesta, quando ciò sia necessario ai fini della decisione, specie con riferimento al rispetto di taluno dei requisiti sopra indicati.

La decisione giudiziaria autorizzatoria della misura deve specificare **almeno i seguenti elementi**:

a) il reato punibile oggetto di indagine e la sua classificazione giuridica, con l'esplicita indicazione delle ragioni su cui si basa la misura;

b) l'identità delle persone indagate e di qualsiasi altra persona interessata dalla misura, se nota;

c) l'entità della misura, specificandone la portata e i motivi relativi al rispetto dei principi direttivi di cui al citato articolo 588-*bis*-*a*.

d) l'unità investigativa della polizia giudiziaria che sarà incaricata dell'intervento;

e) la durata della misura;

f) la forma e la frequenza con cui il richiedente informerà il giudice in merito ai risultati della misura;

g) la finalità perseguita con la misura;

h) il soggetto obbligato all'esecuzione della misura, se noto, con espressa menzione dell'obbligo di collaborazione e segretezza, se del caso, a pena di incorrere nel reato di disobbedienza.

In base all'art. 588-*bis*-*e* c.p.p., la **durata** delle misure in esame è quella specificata per ciascuna di esse e non possono eccedere il tempo essenziale per l'accertamento dei fatti. La misura può essere prorogata, con atto motivato, dal giudice competente, d'ufficio o previa istanza motivata del ricorrente, purché sussistano le cause che l'hanno motivata. Decorso il termine per il quale la misura è stata concessa, senza che vi sia stata proroga, o, in caso, terminata la proroga, la misura cessa a tutti gli effetti. Dacché, tutta questa parte della disciplina tratta di principi comuni ogni forma di intercettazione non viene stabilito un limite temporale unitario: nei capitoli successivi del medesimo titolo sono indicati limiti specifici.

L'art. 588-*bis*-*f* disciplina la **richiesta di proroga**, da indirizzarsi a cura del PM o della polizia giudiziaria al giudice competente con congruo anticipo rispetto alla scadenza del termine inizialmente accordato. Essa, in ogni caso, deve contenere: una relazione dettagliata del risultato della misura e le ragioni che ne giustificano la prosecuzione. La disposizione prevede che entro due giorni dalla presentazione dell'istanza, il giudice decida con ordinanza motivata sulla cessazione della misura o sulla relativa proroga; ai fini della decisione, il giudice può richiedere chiarimenti o maggiori informazioni. Una volta concessa la proroga, il relativo computo decorre dalla data di scadenza del termine della misura accordata.

L'art. 588-*bis-g* sul **controllo della misura**, prevede che la polizia giudiziaria informi il giudice istruttore in merito all'andamento e ai risultati della stessa, con le modalità e la periodicità da questi stabilite e, comunque, quando per qualsiasi motivo essa venga interrotta. Ai sensi dell'articolo 588-*bis-j* il giudice ordina la **cessazione della misura** quando vengono meno le circostanze che ne avevano giustificato l'adozione o quando risulti evidente che con essa non si ottengono i risultati previsti e, in ogni caso, quando è trascorso il periodo per il quale è stata autorizzata.

L'art. 588-*bis-k* disciplina la **distruzione delle registrazioni**, prevedendo che, una volta chiuso il procedimento tramite provvedimento definitivo, viene ordinata la cancellazione e lo smaltimento delle registrazioni originali eventualmente contenute nei sistemi elettronici e informatici utilizzati per l'esecuzione della misura. Una copia deve essere conservata sotto custodia del *Letrado de la Administración de Justicia* (Segreteria legale dell'Amministrazione della giustizia). Viene ordinata la distruzione delle copie conservate una volta trascorsi cinque anni dall'esecuzione della pena o quando il reato o la pena sono prescritti, o quando il caso è stato archiviato o l'imputato è stato assolto, a condizione che, a giudizio del Tribunale, non sia necessario conservarle. I tribunali indirizzano alla polizia giudiziaria gli ordini necessari all'esecuzione della distruzione.

Nei capitoli successivi, introdotti nella *Ley de Enjuiciamiento Criminal* , si entra nel dettaglio delle specifiche discipline. In particolare, quella concernente l'**intercettazione di comunicazioni telefoniche e telematiche** è recata dal Capitolo V, Titolo VIII, Libro II, c.p.p., articolato in **3 sezioni**:

- **Sezione 1, *Disposizioni generali***, articoli da 588-*ter-a* (Presupposti) a 588-*ter-i* (Accesso delle parti alle registrazioni);
- **Sezione 2, *Inclusione nel procedimento di dati di traffico telematico o connessi***, articolo 588-*ter-j* (Dati contenuti negli archivi automatizzati dei fornitori di servizi);
- **Sezione 3, *Accesso ai dati necessari all'identificazione degli utenti, dei terminali e dei dispositivi di connettività***, articoli da 588-*ter-k* (Identificazione tramite numero IP) a 588-*ter-m* (Identificazione di titolari o terminali o dispositivi di connettività).

Nel disciplinare i **Presupposti**, l'art. 588-*ter-a* dispone che l'autorizzazione all'intercettazione di comunicazioni telefoniche e telematiche possa essere concessa solo quando l'indagine abbia ad oggetto uno dei reati di cui all'art. 579, co. 1, c.p.p. (ovvero: reati dolosi puniti con la pena nel limite massimo della reclusione non inferiore a tre anni; reati commessi all'interno di un gruppo o organizzazione criminale; reati di terrorismo), ovvero reati commessi tramite strumenti informatici o di qualunque altra tecnologia dell'informazione, comunicazione o servizio di comunicazione.

Quanto all'**ambito di applicazione**, l'art. 588-*ter-b* specifica che i terminali o i mezzi di comunicazione soggetti a intercettazione devono essere quelli utilizzati abitualmente o occasionalmente dalla persona indagata. Il provvedimento assunto

in via giudiziaria può autorizzare l'accesso al contenuto delle comunicazioni e ai dati del traffico elettronico o ai dati associati al processo di comunicazione, nonché a quelli che si producano indipendentemente dal fatto che sia stabilita o meno una comunicazione concreta, alla quale la persona indagata partecipa, sia come mittente che come destinatario, e può riguardare i terminali o i mezzi di comunicazione di cui l'indagato è titolare o fruitore. Anche i terminali o i mezzi di comunicazione della vittima possono essere intercettati quando è prevedibile un grave rischio per la sua vita o la sua integrità. Per 'traffico elettronico' o 'dati associati' si intendono tutti i dati generati a seguito dell'effettuazione di una comunicazione attraverso una rete di comunicazione elettronica, della sua messa a disposizione dell'utente, nonché della fornitura di un servizio di informazione o comunicazione telematica di analoga natura.

In base all'art. 588-*ter-c*, l'intercettazione di **comunicazioni emesse da terminali o mezzi di comunicazione telematica appartenenti a una terza persona** può essere accordata a condizione che vi sia evidenza che il soggetto indagato se ne serva per trasmettere o ricevere informazioni, oppure che il titolare collabori con la persona indagata per i suoi scopi illeciti o tragga vantaggio dalla sua attività. L'intercettazione può essere autorizzata anche quando il dispositivo oggetto di indagine sia utilizzato dolosamente da terzi per via telematica, all'insaputa del suo titolare.

Ai sensi dell'articolo 588-*ter-d*, la **richiesta di autorizzazione giudiziale** deve contenere, **oltre ai requisiti di cui al citato art. 588-*bis-b*, i seguenti**:

- l'identificazione del numero di abbonato, del terminale o dell'etichetta tecnica;
- l'identificazione del collegamento oggetto dell'intervento o
- i dati necessari all'identificazione del mezzo di telecomunicazione in questione.

Per determinare la **portata della misura**, la richiesta di autorizzazione giudiziale può avere ad oggetto uno dei seguenti estremi:

a) la registrazione del contenuto della comunicazione, con indicazione della forma o del tipo di comunicazioni che interessa;

b) la conoscenza della sua origine o destinazione, nel momento in cui viene effettuata la comunicazione;

c) l'ubicazione geografica dell'origine o la destinazione della comunicazione;

d) la conoscenza di altri dati di traffico associati o non associati ma con valore aggiunto alla comunicazione. In tal caso, la richiesta specificherà i dati concreti che si devono ottenere.

In **caso di urgenza**, quando le indagini siano svolte per accertare reati riconducibili all'azione di **bande armate** o di **elementi terroristici** e ricorrano fondati motivi che rendono indispensabile la misura dell'intercettazione di comunicazioni telefoniche o telematiche, si prevede che la misura possa essere ordinata dal **Ministro dell'Interno** o, in mancanza, dal Segretario di Stato per la Sicurezza. In tal caso, il provvedimento è immediatamente comunicato al giudice competente e, comunque, entro il termine massimo di 24 ore, con l'indicazione

delle ragioni che hanno motivato l'adozione della misura, l'azione intrapresa, le modalità con cui è stata eseguita e il relativo esito. Entro il termine massimo di 72 ore decorrenti dal momento in cui è stata disposta la misura, il giudice competente è chiamato a revocarla ovvero a confermarla con provvedimento motivato.

L'art. 588-*ter-e* proclama l'**obbligo di collaborazione** dei fornitori di servizi di telecomunicazioni, di accesso a una rete di telecomunicazioni o di servizi della società dell'informazione, nonché di qualunque persona contribuisca a facilitare le comunicazioni telefoniche o con qualsiasi altro mezzo o sistema di comunicazione telematica, logica o virtuale. Tali soggetti sono tenuti a fornire al giudice, al PM e agli agenti di polizia giudiziaria preposti all'esecuzione del provvedimento, l'assistenza e la collaborazione necessarie ad agevolare l'adempimento degli ordini di intervento nelle telecomunicazioni. I soggetti obbligati alla prestazione della collaborazione sono tenuti all'osservanza del segreto sulle attività richieste dalle autorità; in caso di inadempienza, possono incorrere nel reato di disobbedienza all'autorità (in base all'art. 556 e ss. c.p., punita, nei casi più gravi, con pena alternativa della multa o della privazione della libertà).

In attuazione del citato art. 588-*bis-g*, in tema di **controllo del provvedimento**, l'art. 588-*ter-f* dispone che la polizia giudiziaria metta a disposizione del giudice, con la periodicità da questi determinata e su diversi supporti informatici, la trascrizione dei brani ritenuti di interesse e le registrazioni integrali effettuate. Devono essere indicate l'origine e la destinazione di ciascuna di esse. Inoltre, l'autenticità e l'integrità delle informazioni trasferite dall'elaboratore centrale ai supporti digitali su cui sono state registrate le comunicazioni devono essere garantite da un sistema avanzato di sigillo o firma elettronica o da un sistema di allerta sufficientemente affidabile.

Ai sensi dell'art. 588-*ter-g*, la **durata massima iniziale** dell'intervento, computato dalla data di autorizzazione giudiziale, è pari a **tre mesi**, **prorogabili per periodi successivi di pari durata sino ad un periodo massimo di diciotto mesi.**

In base all'art. 588-*ter-h*, per motivare la **richiesta di proroga** la polizia giudiziaria fornisce, ove opportuno, la trascrizione dei passaggi delle conversazioni da cui si desumono informazioni rilevanti ai fini della decisione sul mantenimento della misura. Prima di emanare il relativo dispositivo, il giudice può richiedere chiarimenti o maggiori informazioni, compreso il contenuto integrale delle conversazioni intercettate.

L'art. 588-*ter-i* disciplina l'**accesso delle parti alle registrazioni**, stabilendo che - venuto meno il segreto ed esaurita la validità della misura di intercettazione - viene consegnata alle parti copia delle registrazioni e delle trascrizioni effettuate. Se nella registrazione sono presenti dati riferiti ad aspetti della vita intima delle persone, verrà consegnata solo la registrazione e la trascrizione di quelle parti che non vi si riferiscono. La mancata inclusione dell'intera registrazione nella trascrizione consegnata deve essere espressamente dichiarata. Una volta esaminate le registrazioni ed entro il termine fissato dal giudice, tenuto conto della mole di informazioni contenute nei supporti, ciascuna delle parti può chiedere l'inclusione

nelle copie di quelle comunicazioni ritenute rilevanti ma che sono state escluse. Il giudice istruttore, udite o esaminate di persona tali comunicazioni, deciderà sulla loro esclusione ovvero inclusione nella causa. Il giudice istruttore notifica alle persone coinvolte nelle comunicazioni intercettate il fatto dell'intercettazione e le informa sulle specifiche comunicazioni alle quali hanno partecipato che ne sono interessate, salvo che ciò sia impossibile, richieda uno sforzo sproporzionato o pregiudichi le future indagini. Qualora la persona notificata lo richieda, le viene fornita copia della registrazione o della trascrizione di tali comunicazioni, a condizione che ciò non pregiudichi il diritto alla riservatezza di altre persone o sia contrario allo scopo del procedimento nel cui ambito è stata adottata la misura dell'intercettazione.

In merito all'**inclusione nel procedimento di dati di traffico telematico o connessi**, l'art. 588-*ter-j* stabilisce che i dati elettronici conservati da prestatori di servizi o soggetti che facilitano la comunicazione in ottemperanza alla normativa sulla conservazione dei dati relativi alle comunicazioni elettroniche o di propria iniziativa per motivi commerciali o di altra natura e che sono legati ai processi di comunicazione, ai fini della loro inclusione nel procedimento, possono essere trasferiti solo con autorizzazione giudiziale. Quando la conoscenza di tali dati è essenziale per l'indagine, è necessario richiedere al giudice competente l'autorizzazione a ottenere le informazioni contenute negli archivi automatizzati dei fornitori di servizi, compresa la ricerca incrociata o intelligente di dati, a condizione che siano specificati la natura dei dati da rendere noti e i motivi che giustificano il trasferimento.

L'**accesso ai dati necessari all'identificazione degli utenti, dei terminali e dei dispositivi di connettività** di cui alla citata **Sezione 3** è disciplinato dagli articoli 588-*ter-k*, 588-*ter-l* e 588-*ter-m*.

L'art. 588-*ter-k* regola **l'identificazione tramite numero IP**, prevedendo che, quando nell'esercizio delle funzioni di prevenzione e accertamento di reati commessi in rete, gli agenti della polizia giudiziaria hanno accesso a un indirizzo IP utilizzato per commettere un reato e non sono disponibili l'identificazione e l'ubicazione dell'apparecchiatura o del corrispondente dispositivo di connettività, né i dati di identificazione personale dell'utente, chiedono al giudice istruttore di richiedere agli agenti soggetti all'obbligo di collaborazione *ex* art. 588-*ter-e*, il trasferimento dei dati che consentono l'identificazione e la localizzazione del terminale o del dispositivo di connettività e l'identificazione del sospettato.

L'art. 588-*ter-l* statuisce in ordine all'**identificazione dei terminali tramite acquisizione dei codici identificativi del dispositivo o dei suoi componenti**, stabilendo che, qualora nell'ambito di un'indagine non fosse stato possibile ottenere un determinato numero di abbonato e ciò sia indispensabile ai fini dell'indagine, gli agenti di polizia giudiziaria possono utilizzare dispositivi tecnici che consentono l'accesso alla conoscenza dei codici di identificazione o etichette tecniche dell'apparato di telecomunicazione o di uno qualsiasi dei suoi componenti, come la numerazione IMSI o IMEI e, in generale, di ogni mezzo tecnico che, secondo lo stato della tecnologia, sia idoneo a identificare

l'apparecchiatura di comunicazione utilizzata o la carta utilizzata per accedere alla rete di telecomunicazioni. Ottenuti i codici identificativi, gli agenti della polizia giudiziaria possono richiedere al giudice competente l'intercettazione delle comunicazioni nei termini stabiliti dall'articolo 588-*ter-d*; la richiesta deve informare il giudice sull'uso dei predetti dispositivi tecnici. Il tribunale, con delibera motivata, accoglie o respinge la richiesta di intercettazione nel termine di cui all'articolo 588-*bis-c*.

In ordine all'**identificazione di titolari o terminali o dispositivi di connettività**, l'art. 588-*ter-m* prevede che, quando il PM o la polizia giudiziaria, nell'esercizio delle loro funzioni, abbiano esigenza di conoscere l'intestatario di un numero telefonico o di qualsiasi altro mezzo di comunicazione, o, viceversa, abbiano bisogno di conoscere il numero telefonico o i dati identificativi di qualsiasi mezzo di comunicazione, possono rivolgersi direttamente ai fornitori di servizi di telecomunicazioni, di accesso a una rete di telecomunicazioni o di servizi della società dell'informazione, i quali saranno tenuti all'adempimento dell'obbligo di fornitura dei dati richiesti, pena la possibilità di incorrere nel già citato reato di disobbedienza.

Il **Capitolo VI**, Titolo VIII, Libro II, c.p.p., racchiude le norme relative a un'altra disciplina specifica, ovvero quella riguardante l'**Acquisizione e registrazione di comunicazioni orali tramite utilizzo di dispositivi elettronici** e si compone degli articoli da 588-*quater-a* a 588-*quater-e*.

L'art. 588-*quater-a* (**Registrazione di comunicazioni orali dirette**) prevede che possano essere autorizzate la **collocazione e l'uso di dispositivi elettronici** che consentano l'acquisizione e la registrazione di comunicazioni orali dirette mantenute dall'indagato, sulla pubblica via o in altro spazio aperto, nel suo domicilio o in qualunque altro luogo chiuso. Gli apparecchi di ascolto e registrazione possono essere collocati sia all'esterno che all'interno del domicilio o luogo chiuso (comma 1). Nel caso in cui sia necessario l'ingresso nel domicilio o in uno qualsiasi degli spazi destinati all'esercizio della riservatezza, la delibera abilitante deve includere i motivi della necessità di accesso a tali luoghi (comma 2). L'ascolto e la registrazione di conversazioni private possono essere integrati con l'**acquisizione di immagini** quando ciò sia espressamente autorizzato dal provvedimento del giudice (comma 3).

L'art. 588-*quater-b* (**Presupposti**) stabilisce che l'utilizzo dei predetti dispositivi deve essere collegato a comunicazioni che possono avvenire in uno o più specifici incontri dell'indagato con altre persone e sulla cui prevedibilità sussistono indizi emersi dall'indagine. Può essere autorizzato **solo in presenza dei seguenti requisiti**:

a) i fatti oggetto di indagine siano costituivi di uno dei seguenti reati (ovvero i reati di cui al menzionato art. 579, co. 1, c.p.p.):

1. reati dolosi puniti con la pena nel limite massimo della reclusione non inferiore a tre anni;

2. reati commessi all'interno di un gruppo o organizzazione criminale;

3. reati di terrorismo;

b) si possa ragionevolmente prevedere che l'uso dei dispositivi fornirà dati essenziali di rilevanza probatoria per l'accertamento dei fatti e l'identificazione dell'autore del reato.

In merito al **contenuto della decisione giudiziale che autorizza la misura**, l'art. 588-*quater-c* precisa che tale decisione, oltre ai requisiti di cui all'art. 588-*bis-c*, deve contenere specifica menzione del luogo o delle dipendenze, nonché degli incontri dell'indagato che saranno sottoposti a sorveglianza.

Rispetto al **controllo della misura** (art. 588-*quater-d*), si prevede che, in ottemperanza a quanto previsto dall'art. 588-*bis-g*, la polizia giudiziaria mette a disposizione dell'autorità giudiziaria il supporto originale o copia elettronica autentica delle registrazioni e delle immagini, alle quali dovrà essere allegata la trascrizione delle conversazioni ritenute di interesse. Il rapporto identifica tutti gli agenti che hanno partecipato all'esecuzione e al monitoraggio della misura.

L'art. 588-*quater-e* dispone in ordine alla **cessazione della misura**, prevedendo che, una volta terminata la misura per i motivi di cui all'art. 588-*bis-j*, la registrazione di conversazioni che possono aver luogo in altri incontri o l'acquisizione di immagini di tali momenti richiedono una nuova autorizzazione giudiziale.

A sua volta, il **Capitolo IX**, Titolo VIII, Libro II, c.p.p., disciplina le ***Registrazioni da remoto su apparecchiature informatiche*** e si compone degli articoli da 588-*septies-a* a 588-*septies-c*.

Nel disciplinare i **presupposti** per l'applicazione della misura, l'art. 588-*septies-a* prevede - al comma 1 - che il giudice competente possa autorizzare **l'utilizzo di dati e codici identificativi, nonché l'installazione di software** che consentano, **da remoto e per via telematica**, **l'esame a distanza**, all'insaputa del titolare o dell'utilizzatore, **del contenuto di un pc, dispositivo elettronico, sistema informatico, strumento di immagazzinamento massivo di dati informatici o banche dati**, purché persegua l'accertamento di uno dei **seguenti reati**:

a) reati commessi in seno ad organizzazioni criminali;

b) reati di terrorismo;

c) reati contro minori o persone con capacità legalmente modificata;

d) reati contro la Costituzione, di tradimento e relativi alla difesa nazionale;

e) reati compiuti tramite strumenti informatici o qualunque altra tecnologia informatica, telematica o di servizio di comunicazione.

In base al comma 2, **il provvedimento giudiziale di autorizzazione deve specificare**:

a) i computer, dispositivi elettronici, sistemi informatici o parte di essi, supporti informatici per l'archiviazione di dati o banche dati, dati o altri contenuti digitali oggetto della misura;

b) la portata della misura, il modo in cui si procederà all'accesso e sequestro dei dati o degli archivi informatici rilevanti per il caso e il software attraverso il quale verrà effettuato il controllo delle informazioni;

c) gli agenti autorizzati all'esecuzione della misura;

d) l'autorizzazione, se del caso, alla realizzazione e conservazione di copie dei dati informatici.

e) le misure necessarie a preservare l'integrità dei dati immagazzinati, nonché per l'inaccessibilità o la cancellazione di tali dati del sistema informatico cui si è avuto accesso.

Quando gli agenti incaricati della registrazione a distanza abbiano motivo di ritenere che i dati ricercati siano conservati in altro sistema informatico o in parte di esso, ne informano il giudice, il quale può autorizzare una **proroga dei termini della registrazione** (comma 3).

Ai sensi dell'art. 588-*septies-c* (Durata), la misura può avere la **durata massima di un mese, prorogabile per periodi uguali fino ad un massimo di tre mesi.**

L'art. 588-*septies-b* disciplina l'**obbligo di collaborazione** dei prestatori di servizi e delle persone indicate nell'articolo 588-*ter-e*, nonché dei titolari o responsabili del sistema informatico o della banca di dati oggetto della misura, i quali sono tenuti a prestare agli inquirenti la necessaria collaborazione per l'attuazione della misura e l'accesso al sistema. Allo stesso modo, i medesimi soggetti sono obbligati a fornire l'assistenza necessaria affinché i dati e le informazioni raccolte possano essere esaminati e visualizzati. Le autorità e gli incaricati dell'indagine possono ordinare a chiunque sia a conoscenza del funzionamento del sistema informatico o delle misure poste a protezione dei dati informatici in esso contenuti, di fornire le informazioni necessarie per il buon esito dell'indagine. Tale disposizione non si applica alla persona indagata, alle persone esentate dall'obbligo di testimoniare per motivi di parentela e a quelle che, ai sensi dell'art. 416, co. 2, c.p.p. non possono testimoniare in virtù del segreto professionale. I soggetti tenuti a prestare collaborazione hanno l'obbligo di mantenere il segreto sulle attività richieste dalle autorità inquirenti.

Rassegna della giurisprudenza in materia di intercettazioni telefoniche precedente alla riforma del 2015

In primo luogo è in alcune sentenze del Tribunale Supremo che compare la definizione di "intercettazione telefonica" (*intervención telefónica*)[8], intesa come "misura strumentale che presuppone una restrizione del diritto fondamentale al segreto delle comunicazioni e che è ordinata dal giudice istruttore […] al fine di captare il contenuto delle conversazioni per l'indagine di delitti precisi e per l'ottenimento, in caso, di determinati elementi probatori". Si tratta perciò di un "mezzo" il cui fine non è il semplice ascolto delle conversazioni, ma la scoperta della commissione di un reato e dei suoi autori e l'ottenimento di elementi probatori da poter utilizzare in una successiva sede processuale. È quindi indispensabile la decisione di un organo giudiziario per la limitazione di un diritto fondamentale garantito dalla Costituzione, che non può essere autorizzata da alcun

[8] STS (Sentenza del Tribunale Supremo) 2093/1994, STS 246/1995 e STS 711/1996.

organo amministrativo (polizia o forze di pubblica sicurezza), con l'eccezione temporanea del ricordato disposto di cui al comma 4 dell'articolo 579 del Codice di procedura penale.

Come detto, i requisiti indispensabili per l'adozione di una tale misura sono stati precisati in diverse sentenze del Tribunale Supremo e del Tribunale Costituzionale, che fanno soprattutto riferimento al cosiddetto "principio di proporzionalità".

Si tratta di un principio che si applica con riferimento a tutti i diritti fondamentali[9] e che implica che ogni decisione limitativa di uno qualunque dei suddetti diritti debba essere adeguatamente argomentata, con motivazioni di fatto e di diritto che potranno essere successivamente valutate dal soggetto interessato, nell'esercizio del suo diritto di difesa, al fine di giudicare la proporzionalità tra la restrizione del diritto e la ragione che l'ha determinata[10].

Ogni ipotesi di reato si basa su un sospetto, come è ovvio, ma in questo caso devono essere presenti degli elementi e dei dati obiettivi, che possono essere mostrati a terzi, e dei fondamenti reali per affermare che è stato, o sta per essere, commesso un reato, al di là di semplici valutazioni soggettive sulla persona indagata.

Il giudice competente dovrà quindi valutare caso per caso ed è compito dell'organo che richiede l'autorizzazione all'uso delle intercettazioni telefoniche (in genere le forze di polizia) fornire dati obiettivi e non semplici supposizioni o congetture; è stato precisato che la decisione del giudice va comunque valutata in una prospettiva *ex ante*, con ponderazione degli elementi esistenti al momento della richiesta, e non deve essere giudicata *ex post*, cioè con giustificazione a posteriori, a seguito dei risultati ottenuti, o meno, con l'uso delle intercettazioni telefoniche[11].

Ulteriori aspetti, introdotti da diverse altre pronunce giurisprudenziali, sono stati: lo spostamento dal "giudizio di idoneità" al "giudizio di necessità", che impone di accertare se esista qualche altro strumento meno invasivo della libertà personale per conseguire lo stesso risultato investigativo; la considerazione della gravità dei reati ipotizzati e della loro rilevanza sociale; l'affermazione del "principio di specialità", in base al quale, in caso di scoperta di reati diversi da quelli per i quali era stata concessa l'autorizzazione alle intercettazioni, è necessario chiedere una nuova autorizzazione per poter indagare formalmente su di essi.

Il giudice istruttore, dopo la sua decisione, ha inoltre il dovere di seguire lo svolgimento delle attività di intercettazione, vigilando affinché la restrizione del diritto fondamentale resti comunque nei limiti costituzionali[12].

In concreto sono stati poi precisati dalla giurisprudenza alcuni aspetti specifici relativi allo svolgimento delle attività di intercettazione, tra i quali vi è l'obbligo di consegnare al giudice le registrazioni originali ed in formato integrale[13], con

[9] STS 55/1996.
[10] STC (Sentenza del Tribunale Costituzionale) 37/1989 e STC 85/1994.
[11] STS 1690/2003.
[12] STC 49/1996.
[13] STC 166/1999, STC 171/1999, STC 299/2000 e STC 14/2001.

connessa esigenza di trascrizione integrale del contenuto delle registrazioni stesse, in modo da evitare "selezioni" o "tagli" preventivi da parte delle autorità di polizia[14]. Altro elemento imprescindibile, basato sul diritto alla difesa della persona indagata, consiste nel dovere di porre a conoscenza dell'interessato tutto il contenuto delle intercettazioni, nel termine massimo di 10 giorni prima della conclusione delle indagini preliminari, e di dar luogo ad un'audizione del soggetto stesso (*audición contradictoria*), innanzi al giudice, prima della conclusione di questa fase del procedimento.

Un'ulteriore importante questione, affrontata sia dal Tribunale Supremo sia dal Tribunale Costituzionale, è quella delle conseguenze giuridiche di un'attività di intercettazione effettuata in modo illecito, cioè in violazione di quanto disposto dalla legge o dalla giurisprudenza consolidata, con riferimento alle prove della commissione di un reato eventualmente ottenute. L'orientamento dominante impone la verifica se esista o meno una causalità diretta e una connessione esclusiva tra l'intercettazione illecita e la prova (o le prove) risultanti a carico dell'indagato; si tratta di un concetto denominato "connessione di antigiuridicità" (*conexión de antijuridicidad*)[15]. In sostanza occorre accertare, caso per caso, se le prove risultanti avrebbero potuto o no essere ottenute senza l'intercettazione illecita; va valutato, in altri termini, se le prove siano state generate unicamente dalle intercettazioni oppure se siano state acquisite anche attraverso altri mezzi[16].

Va inoltre segnalato che anche l'assenza di una normativa più dettagliata sugli aspetti procedurali menzionati fu oggetto di critiche da parte dei giudici, che censurarono le lacune esistenti nelle disposizioni vigenti, invitando il legislatore ad approvare al più presto una normativa più adeguata in materia[17], salvo essere ascoltati solo dopo diversi anni.

Nel 2009 il Tribunale Costituzionale ha ricostruito in dettaglio il quadro dottrinale in materia di intercettazioni[18]. Esso ha tra l'altro ricordato che, a partire dalla sentenza 49/1999, il medesimo Tribunale ha ripetutamente affermato che formano parte del contenuto essenziale dell'articolo 18.3 della Costituzione le esigenze di motivazione delle risoluzioni giudiziarie che autorizzano l'intercettazione o la sua proroga. Appare necessario, per il Tribunale Costituzionale, esplicitare al momento dell'adozione della misura tutti gli elementi indispensabili per realizzare il giudizio di proporzionalità e per rendere possibile il controllo successivo, nel rispetto del diritto di difesa del soggetto interessato, proprio perché, per la stessa finalità della misura dell'intercettazione, la difesa non può essere presente al momento dell'adozione della misura stessa. Nella medesima pronuncia, il Tribunale ha sottolineato che, nel caso in cui la conoscenza del reato derivi da precedenti investigazioni di polizia, appare necessario che siano portati a conoscenza del giudice i dettagli in merito a tali investigazioni e ai relativi risultati,

14 STS 2249/1994.
15 STC 171/1999 e STC 50/2000.
16 STS 330/2003 e STS 1690/2003.
17 STS 184/2003 in particolare.
18 STC 197/2009.

anche se provvisori, che egli potrà valutare prima di concedere l'autorizzazione all'intercettazione.
Il Tribunale Supremo ha inoltre sancito la legalità del sistema di intercettazioni SITEL[19]. Il Tribunale ha infatti affermato che tale sistema offre le necessarie garanzie derivanti proprio dalle sue caratteristiche di centralizzazione, sicurezza ed automazione[20]. Nel gennaio 2010 l'Agenzia spagnola di protezione di dati (AEPD) ha peraltro confermato che SITEL garantisce i principi di esattezza e d'integrità previsti dalla normativa vigente in materia di protezione dei dati[21].

[19] Il *Sistema Integrado de Interceptación Telefónica* (SITEL) è un sistema informatico di intercettazioni telefoniche del Ministero dell'interno. In sostanza, esso centralizza le informazioni ricevute dalle attività di intercettazioni eseguite dai diversi operatori di telefonia. Tale sistema è stato al centro di una polemica incentrata su un possibile controllo non autorizzato delle conversazioni di alcuni esponenti politici.
[20] STS 1078/2009.
[21] Si veda il comunicato "*La AEPD concluye la inspección sobre SITEL*", emesso dalla medesima Agenzia (19 gennaio 2010).

Stati Uniti d'America

Il quadro normativo

Negli Stati Uniti d'America la materia delle intercettazioni è disciplinata, a livello federale, dal *Title III* dello *Omnibus Crime Control and Safe Streets Act* del 1968, confluito nello *U.S. Code*[22]. Al di sopra del livello federale, il fondamento costituzionale dell'istituto deve essere rintracciato nel IV Emendamento, ai sensi del quale "il diritto dei cittadini di godere della sicurezza personale, della loro casa, delle loro carte e dei loro beni, nei confronti di perquisizioni e sequestri ingiustificati non potrà essere violato; e non si emetteranno mandati giudiziari se non su fondati motivi sostenuti da giuramento o da dichiarazione solenne e con descrizione precisa del luogo da perquisire e delle persone da arrestare o delle cose da sequestrare". A ben vedere la Corte Suprema nel 1967 ha ritenuto che la protezione nei confronti di perquisizioni e sequestri ingiustificati prevista dal IV Emendamento dovesse trovare applicazione anche all'intercettazione delle comunicazioni e a tutte le conversazioni per le quali una persona ha una ragionevole aspettativa di *privacy* [23].

La prima regolazione normativa delle intercettazioni telefoniche avvenne nel contesto del *Federal Communication Act* del 1934.

Nella loro concreta applicazione, i testi normativi di riferimento concernenti le intercettazioni sono stati pertanto oggetto di una cospicua giurisprudenza che ne ha integrato il contenuto sostanziale.

La disciplina dettata dalla normativa federale rappresenta una specie di minimo comune denominatore cui tutti i singoli Stati devono adeguare la propria disciplina interna, nel senso che nessuno di essi può permettere l'accesso a comunicazioni telefoniche, orali o elettroniche sulla base di giustificazioni meno forti di quelle richieste dalla legge federale. I singoli Stati hanno invece facoltà, al contrario, di **imporre criteri ancora più stringenti di quelli federali** per autorizzare le intercettazioni, o addirittura di vietarle del tutto, o di non dotarsi di proprie norme in materia. L'ultima edizione attualmente disponibile del Rapporto sulle intercettazioni curato dalle *United States Courts*, lo *Wiretap Report* per l'anno 2021 (diffuso a giugno 2022) riferisce che sono 48 le giurisdizioni che hanno leggi le

[22] In particolare nel *Title 18 (Crimes and Criminal Procedure)*, sezioni 2510-2523, la cui versione vigente è stata oggetto nel corso del tempo di una serie di interventi legislativi: lo *Electronic Communications Privacy Act (ECPA)* del 1986, il *Communications Assistance to Law Enforcement Act (CALEA)* del 1994, *l'Antiterrorism and Effective Death Penalty Act ("Antiterrorism Act")* del 1996, lo *USA Patriot Act del 2001*, (Pub. L. 107-56; 10/26/01), lo *USA Patriot Additional Reauthorization Amendments Act* del 2006, il *FISA (Foreign Intelligence Surveillance Act) Amendments Act* del 2008, il *FISA Sunsets Extension Act* del 2011 e il *Patriot Sunsets Extension Act* del 2011, il *CLOUD Act* del 2018.

[23] Si vedano le sentenze sui casi Berger vs. New York, 1967, e Katz vs. United States, 1967.

quali consentono all'autorità giudiziaria di emanare provvedimenti di sorveglianza telefonica, orale o elettronica (il Governo federale, quarantaquattro Stati, nonché il *District of Columbia*, le Isole Vergini e Portorico).

Limitando l'esame alla **legislazione federale**, si osserva che sostanzialmente essa regola due fenomeni di origine diversa, con l'obiettivo di bilanciare le esigenze poste da entrambi. A fine anni Sessanta il fondamentale *Title III* dello *Omnibus Crime Control and Safe Streets Act* fu approvato a seguito di inchieste e studi comprovanti il largo uso delle intercettazioni da parte di soggetti pubblici e privati senza il consenso degli interessati, nonché la sempre più frequente utilizzazione di esse nei processi giudiziari e nei procedimenti amministrativi. Tale intervento legislativo, quindi, si pose a garanzia di diritti fondamentali della persona. Nei decenni successivi, piuttosto, acquisirono grande rilievo le problematiche connesse agli strumenti di repressione dei reati. Di intercettazioni nella lotta contro i reati comuni, e della loro divulgazione, si occupò il *Violent Crime Control and Law Enforcement Act* del 1994. Quanto alla sicurezza nazionale, la regolazione introdotta nel 1978 con il *Foreign Intelligence Surveillance Act* (noto con l'acronimo FISA) è stata aggiornata da interventi legislativi che, con finalità anti-terrorismo e con prevalente riguardo alle attività clandestine condotte da entità straniere o da loro agenti sul territorio nazionale, hanno conferito alle autorità di polizia poteri di sorveglianza sulle comunicazioni. Testo fondamentale, al riguardo, è il già citato *Patriot Act* del 2001, poi modificato nel 2002 dallo *Homeland Security Act* e oggetto di ulteriori revisioni in occasione dei parziali *enactements* degli anni successivi.

La legislazione sulle intercettazioni, inoltre, si è evoluta per tenere il passo con l'evoluzione delle tecnologie. Mentre il *Title III* dello *Omnibus Crime Control and Safe Streets Act* del 1968 riguardava soltanto comunicazioni telefoniche e orali, lo ECPA del 1986 incluse nella regolazione le comunicazioni elettroniche, la conservazione dei dati, i registri elettronici e i sistemi di tracciamento. Nel 2001, il *Patriot Act* estese i poteri pubblici di sorveglianza anche a Internet. I mutamenti sopravvenuti nel settore delle telecomunicazioni degli anni '90 del secolo scorso, invero, concernettero non soltanto gli aspetti tecnologici delle reti ma anche l'assetto istituzionale ed economico dei gestori, con particolare riguardo alle liberalizzazioni e alle privatizzazioni. Si avvertì perciò la necessità di preservare, nei nuovi contesti, la possibilità per le autorità preposte alla tutela dell'ordine pubblico di sottoporre a controlli le comunicazioni private, condizionata alla sussistenza di specifici requisiti e sottoposta ad attività conoscitive e di vigilanza dei poteri pubblici.

La disciplina federale delle intercettazioni

Partendo da una serie di definizioni, la normativa statunitense stabilisce all'articolo 2510 dello *U.S. Code* che per intercettazione deve intendersi l'acquisizione del contenuto di comunicazioni, sia esso espresso dalla voce umana oppure da immagini, segni, scritti, suoni, mediante l'utilizzazione di qualsiasi dispositivo, elettronico o meccanico.

In linea generale, è vietato effettuare (o tentare di effettuare) intenzionalmente intercettazioni di comunicazioni qualunque sia la modalità prescelta: orale, via cavo o elettronica (*U.S. Code*, Titolo 18, sezione 2511, paragrafo 1, lettera a). **Sono lecite soltanto le autorizzazioni a fini di giustizia** (*U.S. Code*, Titolo 18, sezione 2516). Esse peraltro devono essere state debitamente autorizzate e devono riferirsi a reati elencati dalla legge, a meno che non siano in corso emergenze, di cui si dirà più avanti.

Ovviamente i fini di giustizia, che sono riconosciuti in primo luogo per il personale dell'amministrazione pubblica che lavora in questo campo, si estendono anche a *provider* e operatori delle telecomunicazioni la cui collaborazione sia richiesta allo scopo di riuscire a realizzare l'intercettazione. Questi ultimi, anzi, sono obbligati a prestare aiuto alle autorità. A tale proposito si segnala l'approvazione nel 2018 del *CLOUD Act*, una legge in base alla quale le autorità degli USA possono imporre ai *provider* del Paese di fornire dati anche se questi ultimi sono immagazzinati all'estero.

Il *CLOUD Act* pertanto riguarda soprattutto i rapporti tra i poteri pubblici degli USA e le compagnie private le cui attività si svolgono in tutto il globo. Non a caso, l'impulso alla regolazione della materia è partito da un contenzioso tra il governo degli Stati Uniti e Microsoft a proposito di dati conservati da quest'ultima nelle sue sedi ubicate in Irlanda.

Si tenga presente che l'applicazione del *CLOUD Act*, una legge che per sua natura ha implicazioni rilevanti rispetto allo stato delle relazioni fra gli USA e i Paesi che ospitano le compagnie private cui si chiede di fornire i dati in loro possesso, può avvenire solo a condizione che le autorità straniere diano il loro consenso. Tale condizione è realizzabile per mezzo di accordi (*agreements*) bilaterali tra gli USA ed il Paese interessato. Di conseguenza, in alcune situazioni il ricorso al *CLOUD Act* è impraticabile e, in ogni caso, è sempre esposto ad incognite che non dipendono dalle autorità degli Stati Uniti. Per giunta, la bilateralità degli accordi comporta che assumere iniziative ai sensi del *CLOUD Act* impegna gli USA alla reciprocità di fronte ad eventuali richieste da parte dell'altro Paese contraente, cosa che può avere i suoi lati negativi e che impone prudenza nello stipulare accordi.

La titolarità del potere di autorizzare le intercettazioni fa capo all'*Attorney General* o ai suoi sottoposti da lui delegati.

L'*Attorney General* è una figura che non trova preciso corrispettivo nell'ordinamento italiano e, pertanto, a volte viene paragonato al Ministro della Giustizia, altre ad un Procuratore Generale. Può essere utile ricordare che l'*Attorney General* è il capo del Dipartimento della Giustizia degli USA, è nominato dal Presidente degli Stati Uniti -con l'approvazione del Senato-, è il principale consigliere del Presidente stesso nelle materie giuridiche ed è membro del *Cabinet of the United States*.

L'*Attorney General* (o il suo delegato) autorizza l'invio di una richiesta per effettuare un'intercettazione, proveniente da un organismo investigativo, ad un giudice federale il quale, a sua volta, emetterà un *intercept order* qualora il ricorso al mezzo di indagine in questione appaia ragionevolmente necessario al fine di perseguire i reati rispetto ai quali le intercettazioni sono ammissibili. La durata massima delle intercettazioni è di trenta giorni, un termine che tuttavia può essere rinnovato in caso di particolari esigenze investigative, aggiungendo un massimo di altri trenta giorni (*U.S. Code*, Titolo 18, sezione 2518, paragrafo 5). Da notare che la richiesta di autorizzazione, possibilmente, dovrebbe riportare i reati per i quali si intendono raccogliere le prove, i motivi dell'inefficacia (già sperimentata oppure ritenuta probabile) delle normali procedure investigative e, infine, modalità di sorveglianza idonee a ridurre al minimo l'accesso a contenuti senza rilevanza probatoria oppure riferiti a soggetti estranei all'indagine, nonché specificare il tipo e la localizzazione degli apparecchi da intercettare. Tuttavia, quando risulta impossibile precisare tipo e localizzazione degli apparecchi da intercettare, possono essere concesse autorizzazioni dette *roving wiretap*, cioè eseguibili su qualsiasi tipo di apparecchiatura di cui si serva la persona da intercettare. Il principio garantista della *minimization* cui si è accennato, ossia della massima riduzione possibile del coinvolgimento nelle intercettazioni di persone estranee ai reati e della salvaguardia della loro *privacy*, è tenuto in elevata considerazione; la controprova di ciò è la complementare *exclusionary rule*, regola in forza della quale l'imputato potrebbe chiedere di dichiarare inutilizzabili tutti i risultati delle comunicazioni intercettate se si dimostrasse che nessuna misura di *minimization* era stata adottata.

Nel lungo elenco di reati in relazione ai quali si possono disporre intercettazioni sono compresi, fra gli altri, l'omicidio, la rapina, l'estorsione, il traffico di stupefacenti, la sottrazione di persona, le molestie ai minori, la cospirazione contro la sicurezza nazionale e, in generale, i reati punibili con la pena capitale o con pene detentive superiori ad un anno (*U.S. Code*, Titolo 18, sezione 2516).

Le situazioni di emergenza in cui si possono effettuare intercettazioni giudiziarie senza attendere la formale autorizzazione attraverso le procedure appena descritte sono: pericoli immediati di morte o di lesioni gravi per una o più persone, attività cospiratorie che minaccino la sicurezza nazionale e attività cospiratorie tipiche della criminalità organizzata (*U.S. Code*, Titolo 18, sezione 2518, paragrafo 7). In queste ipotesi emergenziali la polizia può intercettare di sua

iniziativa ma deve nel frattempo preparare una richiesta di autorizzazione da sottoporre al giudice competente entro quarantotto ore dall'inizio delle intercettazioni. In attesa del provvedimento giudiziario, le intercettazioni potranno andare avanti fino al raggiungimento del loro obbiettivo (e non oltre), ma se l'autorizzazione viene negata dal giudice devono cessare immediatamente.

Il *Foreign Intelligence Surveillance Act* (FISA), per le operazioni nei confronti di agenti o potenze stranieri, reca disposizioni diverse rispetto alla disciplina dell'intercettazione giudiziaria. In questi casi, essendo in gioco la sicurezza nazionale, al fine di procedere alle intercettazioni non occorre dimostrare l'imminenza di crimini ad opera dei destinatari della misura di contrasto, bensì il fatto che si tratti di stranieri o di persone che si sono messe al servizio di potenze straniere, che la sorveglianza è per motivi di *intelligence* e che essa avverrebbe avendo cura di limitarsi al minimo indispensabile (*U.S. Code*, Titolo 50, sezione 1804). Vi è motivo di ritenere, inoltre, che nella lotta contro il terrorismo internazionale gli Stati Uniti facciano uso anche di virus informatici aventi funzioni di captatori informatici (*trojan*), che invadono dispostivi telefonici[24]. La durata prevista dell'intercettazione disposta per motivi di *intelligence* va indicata nella richiesta di autorizzazione; nella prassi, spesso varia da novanta a centoventi giorni e può essere allungata per mezzo di un formale rinnovo. Allo scopo di ottenere l'autorizzazione, il Dipartimento di Giustizia si rivolge ad un organismo creato appositamente per le questioni relative alla sicurezza esterna, la *Foreign Intelligence Surveillance Court* (*FISC*).

L'ordinamento statunitense dedica altresì ulteriori disposizioni ai dati del traffico delle comunicazioni, vale a dire i dati sulle comunicazioni in arrivo o in partenza presso una determinata utenza (*addressing information*). Questi aspetti vengono disciplinati da articoli generalmente conosciuti con gli appellativi di *Pen Registers and Trap and Trace Devices Statutes* (*U.S. Code*, sezioni 3121-3127). Per le *addressing information* la richiesta degli organi inquirenti, motivata unicamente sulla base della presumibile rilevanza delle intercettazioni per le indagini in corso, non soggiace a valutazioni di merito ai fini dell'autorizzazione e l'autorità giudiziaria – la stessa che ha giurisdizione sul reato oggetto delle indagini - si limita ad accertare la conformità ai requisiti di legge. La durata massima delle intercettazioni così autorizzate è di 60 giorni, prorogabili con successivi rinnovi.

Al di fuori delle ordinarie procedure di autorizzazione, del rispetto della casistica dei reati e delle situazioni emergenziali o particolari di cui sopra, ogni intercettazione giudiziaria risulterebbe inutilizzabile nel processo -salvo consenso da parte del soggetto intercettato, e costituirebbe reato.

[24] Cfr. D. E. Sanger, *U.S. Unleashes Digital Arsenal in War With ISIS*, <<New York Times>>, 24/25 aprile 2016, nonché la relazione svolta al seminario della Scuola Superiore della Magistratura dall'alto magistrato Giovanni Salvi, *Uno sguardo comparatistico sul bilanciamento tra libertà delle comunicazioni ed esigenze della sicurezza nazionale ed internazionale*, Scandicci, 11 maggio 2016.

La questione dell'utilizzabilità o no di comunicazioni relative a reati diversi da quelli cui si riferisce l'autorizzazione all'intercettazione si è posta nella giurisprudenza. L'indirizzo finora prevalso è in favore dell'utilizzabilità, sulla base del principio della *plain view*, che è accettato anche dall'interpretazione corrente del IV Emendamento. Si è argomentato che analogamente al caso in cui un agente di polizia legittimamente presente in un luogo veda una cosa sequestrabile e la acquisisca, così un agente il quale stia effettuando un'intercettazione debitamente autorizzata continui a tenere acceso il registratore qualora gli capiti di ascoltare una spontanea dichiarazione indiziante di reati diversi da quelli per i quali si intendeva indagare. L'accidentalità della scoperta è dunque requisito per la sua utilizzabilità: le evidenze emerse dall'intercettazione, infatti, sono inutilizzabili qualora l'autorizzazione relativa ad un reato fosse stata usata come sotterfugio per fare intercettazioni riguardanti un reato diverso, rispetto al quale l'autorizzazione ad intercettare non sarebbe stata concessa[25].

Dopo la conclusione delle intercettazioni, le procedure di conservazione dei dati raccolti sono piuttosto rigide, a tutela della riservatezza. L'organo che ha eseguito l'intercettazione redige un inventario contenente gli estremi del provvedimento autorizzativo e indicazioni su come è stato concretamente svolto il lavoro. Il *prosecutor* deve consegnare al più presto le registrazioni e i relativi supporti materiali al giudice, che pone il tutto sotto sigillo. Se il supporto materiale rimane temporaneamente incustodito, l'intercettazione non viene riconosciuta come prova. L'eventuale continuazione abusiva delle intercettazioni oltre la scadenza dei termini può dare luogo a un'azione civile nei confronti di chi non si è fermato. Il disvelamento (*discovery*) dei testi delle intercettazioni avviene non prima del rinvio a giudizio, su richiesta espressa dell'imputato. La *discovery* avviene mediante consegna diretta al difensore dell'imputato.

In caso di violazione dei divieti di intercettazione posti dalla legge, le sanzioni possono essere di tipo pecuniario, o carcerario fino ad un massimo di cinque anni, o di entrambi i generi insieme (*U.S. Code*, Titolo 18, sezione 2510, paragrafo 4). Si anticipa qui che il codice statunitense prevede sanzioni addizionali per la divulgazione e l'uso illegale delle comunicazioni intercettate.

La divulgazione delle intercettazioni

A norma di legge, sono proibiti la divulgazione (*disclosure*) intenzionale e l'uso intenzionale del contenuto di comunicazioni acquisito sia mediante intercettazioni effettuate illecitamente (*U.S. Code*, Title 18, articolo 2511, lettera d), sia mediante

[25] Per un contributo di dottrina in tema di utilizzabilità dell'intercettazione relativamente a reati diversi da quelli previsti nell'autorizzazione, cfr. V. FANCHIOTTI, *Le intercettazioni negli Stati Uniti d'America*, <<Archivio della nuova procedura penale>>, fascicolo 1/2017, pp. 6-11.

intercettazioni autorizzate (*U.S. Code*, Title 18, articolo 2511, lettera e). Il concetto di uso comprende le attività che non consistono nella divulgazione.

Ad esempio, ricadono nella categoria dell'uso l'acquisizione illecita di informazioni commerciali per trarne vantaggi economici, di codici di accesso a sistemi informatici, oppure la minaccia di divulgare informazioni allo scopo di influenzare o ricattare qualcuno.

Non costituisce reato, però, divulgare o usare contenuti di comunicazioni facilmente accessibili (*readily accessible*), né contenuti che, quale che fosse in origine il loro grado di accessibilità originaria, nel frattempo sono diventati di pubblico dominio.

Nel caso di intercettazioni illegali, la loro divulgazione costituisce un reato addizionale rispetto all'acquisizione dei contenuti. Per le violazioni dei divieti in materia, è prevista una pena detentiva determinata nel massimo di 5 anni o l'irrogazione di un'ammenda, o entrambe le cose. L'ammenda da infliggere alle organizzazioni può essere doppia di quella da infliggere alle persone fisiche.

La divulgazione e l'uso sono punibili se l'imputato era consapevole -o aveva motivo di esserlo- che le informazioni in oggetto era state ottenute illegalmente. È altresì punibile se era ragionevole immaginare che la provenienza fosse illecita. Quando si tratta di intercettazioni giudiziarie legittime, l'imputato di divulgazione o di uso è punibile se è consapevole appunto del fatto che i contenuti dell'intercettazione sono legati a un'indagine giudiziaria. Colui che divulga o usa informazioni raccolte mediante intercettazioni eseguite nell'ambito dell'indagine giudiziaria, inoltre, è punibile se la sua intenzione è di interferire con l'indagine.

A fronte dei divieti e delle conseguenti sanzioni, la legge ammette alcune eccezioni e pone limitazioni ai divieti stessi. Una esimente è costituita dal carattere consensuale delle intercettazioni (*U.S. Code*, Titolo 18, sezione 2511, paragrafo 2, lettera c e lettera d), che sussiste quando una delle parti della comunicazione abbia prestato il previo consenso (tipicamente, in quanto tale soggetto agisca *under color of law* oppure intenda cooperare segretamente con le autorità nel contesto di indagini di polizia). Un'altra esimente vale per le attività di *foreign intelligence* condotte a norma di legge federale (ancora *U.S. Code*, Titolo 18, sezione 2511). Un rilevante limite al divieto di divulgazione, inoltre, è stato individuato dalla Corte Suprema sulla base del principio costituzionale della libertà di espressione. L'esigenza di bilanciare diversi principi e valori di rango costituzionale -la libertà di informazione e di espressione da un lato, l'amministrazione della giustizia e la riservatezza individuale dall'altra- nel corso di decenni ha stimolato l'elaborazione alcune regole di salvaguardia della funzione giornalistica, in relazione ai casi in cui lo svolgimento della relativa attività venga in conflitto con gli altri interessi tutelati. La *policy* adottata dal Dipartimento della Giustizia fin dal 1980 (trasposta nel *Code of Federal Regulations*) individua, sotto questo profilo, un punto di

equilibrio statuendo che <<l'azione punitiva dello Stato non può essere posta in essere in modo da limitare il dovere del cronista di riportare in maniera ampia, per quanto possibile, notizie su questioni, anche controverse, di pubblico interesse>>.

Nella sentenza emessa nel 2001 relativa al caso giudiziario Bartnicki v. Vopper (e nelle opinioni concorrenti), pur senza affermare una generale esimente dei media rispetto al divieto legislativo, è stato assegnato rilievo, ai fini della decisione, al contenuto delle informazioni divulgate, al carattere notorio della persona coinvolta e al grado di riservatezza su cui questa avrebbe potuto fare affidamento in relazione al mezzo di comunicazione utilizzato.

Di questa attenta ponderazione di interessi è indice anche la previsione che condiziona l'emanazione dei provvedimenti adottati nei confronti di giornalisti (ad esempio, per convocarli in qualità di testimoni in procedimenti giudiziari o per intercettarne le comunicazioni) alla previa autorizzazione dell'*Attorney General*.

La questione del diritto di cronaca -che indubbiamente ha punti di contatto con la disciplina delle intercettazioni- è tuttora aperta soprattutto riguardo alla sussistenza o no di un'immunità (*privilege*) dei giornalisti rispetto all'obbligo di rivelare le proprie fonti, che in caso affermativo deriverebbe dall'enunciazione costituzionale della libertà di manifestazione del pensiero recata dall'Emendamento I della Costituzione degli Stati Uniti. In proposito vi sono orientamenti legislativi e giurisprudenziali discordanti. La Corte Suprema affrontò il problema nel 1972, in occasione del caso *Branzburg vs. Hayes*, i suoi giudici si divisero e l'esito, raggiunto a maggioranza di cinque contro quattro, non diventò mai un riferimento comune per tutte le corti di rango inferiore che da allora si occuparono di casi simili, né la Corte Suprema si pronunciò nuovamente. In ambito politico-legislativo, attualmente non esiste una legge federale.

Nel 2021 i senatori Wyden e Raskin, democratico il primo e repubblicano il secondo, presentarono insieme un *Press Act*, che però non passò.

Tuttavia dopo la vicenda del 1972, a livello di singoli Stati, una quarantina di essi ha approvato statuti, detti *shield laws*, che in minore o maggiore misura proteggono le fonti giornalistiche ovvero danno ai giornalisti il diritto di non svelare le proprie fonti[26].

In ogni caso è opportuno osservare che, tradizionalmente, negli Stati Uniti i problemi di fughe di notizie (*leaks*) attinenti ad intercettazioni legate alle inchieste giudiziarie non sono paragonabili a quelli che si registrano in Italia.

[26] In proposito, si può trovare un compendio aggiornato della normativa dei singoli Stati in questo campo, a cura del *Reporters Committee for Freedom of the Press*, presso il sito www.rcfp.org/reporters-privilege/

Il caso di Julian Assange e delle notizie da lui diffuse tramite Wikileaks, che è esploso nel 2010 e che ha avuto e ha tuttora ampia risonanza internazionale, al momento è da considerarsi un caso di diffusione di documenti riservati piuttosto che di violazione della normativa sulle intercettazioni.

La differenza dipende da un insieme di fattori. Il primo è che i numeri delle intercettazioni giudiziarie negli USA sono sensibilmente più bassi di quelli italiani (come si dirà più ampiamente in un paragrafo dedicato ai dati statistici, che completerà la presente esposizione). Il secondo fattore è che, a detta di molti osservatori e come incidentalmente si è mostrato anche in queste pagine, negli Stati Uniti la sensibilità per la riservatezza è più sviluppata. Un terzo fattore potrebbe risiedere nella diversità delle procedure delle intercettazioni giudiziarie statunitensi rispetto a quelle italiane, specialmente nelle fasi successive al termine delle intercettazioni stesse.

Alcuni dati

Ai sensi dello *U.S. Code*, Titolo 18, sezione 2519, a giugno di ogni anno *l'Administrative Office* delle *United States Courts* trasmette al Parlamento (*Congress*) una relazione, dal titolo *Wiretap Report* seguito dall'anno di riferimento. Lo *Wiretap Report* fornisce i dati sulle intercettazioni giudiziarie telefoniche (*wire intercepts*), orali (*oral*) o elettroniche (*electronic*). Il rapporto riferisce intorno alle richieste di intercettazioni giudiziarie, alle autorizzazioni concesse o negate e ai rinnovi, e offre informazioni supplementari su arresti e condanne portati a termine durante l'anno di riferimento che costituiscano il risultato di intercettazioni svoltesi in anni precedenti. Lo *Wiretap Report* ha il formato di un insieme di dati statistici, corredati da un riassunto delle evidenze salienti e da analisi. Lo *Wiretap Report* annuale non comprende le intercettazioni regolate dal *Foreign Intelligence Surveillance Act*, ovvero le intercettazioni non giudiziarie. Occorre precisare altresì che i dati riportati nello *Wiretap Report* si riferiscono esclusivamente alle comunicazioni effettivamente avvenute, mentre non includono le chiamate senza risposta e le geolocalizzazioni. La serie dei rapporti annuali ebbe inizio nel 1997 e i testi sono disponibili online all'indirizzo www.uscourts.gov/statistics-reports/analysis-reports/wiretap-reports . Il più recente, al momento, è perciò lo *Wiretap Report* relativo all'anno 2021, uscito nel 2022, e il prossimo è previsto per il giugno 2023.

Complessivamente, dall'esame dei rapporti annuali, emerge che il ricorso allo strumento delle intercettazioni è molto più limitato che in Italia e che la sua diffusione negli Stati Uniti è tutt'altro che uniforme. I due tratti appena indicati sono entrambi piuttosto costanti anche nel lungo termine, ovvero sin da quando si compiono le rilevazioni che vengono trasfuse negli *Wiretap Report*.

Prima di illustrare le cifre delle intercettazioni giova ricordare che la popolazione degli Stati Uniti d'America nel 2021, secondo le stime ufficiali, era di 331,9 milioni di persone.

Lo *Wiretap Report 2021* informa che in tale anno furono autorizzate 2.245 intercettazioni telefoniche, una cifra in calo del 6% rispetto a quelle del 2020. Nel 94% dei casi le intercettazioni sono state effettuate su dispositivi portatili. Il fenomeno delle intercettazioni si concentra soprattutto in sei Stati che, messi insieme, rappresentano circa l'80% del totale: nell'ordine, essi sono California, New York, Nevada, North Carolina, Colorado e Florida.

Tra le tipologie di reato interessate dalle investigazioni per mezzo di intercettazioni telefoniche, primeggiano quelle legate alla droga (*drug offences*), che sono la maggioranza assoluta, arrivando al 79%. Seguono le cospirazioni (*conspiracy*) con l'11% e l'insieme di omicidi e aggressioni fisiche (*homicide and assault*) con il 5%.

Comunemente si ritiene che il primato delle intercettazioni per *drug offences* sia il motivo per il quale in cima alla classifica degli Stati dove avvengono le intercettazioni stesse ci sia la California, che è molto colpita da reati di quel genere.

Nel 2021 gli arrestati a seguito di *wiretaps* sono stati 8.314, con un sensibile incremento (26%) rispetto al 2020. Nel 2021 le condanne originate da investigazioni condotte con l'ausilio di *wiretaps* sono state 946, un numero più che doppio rispetto all'anno 2020.

Riguardo alla durata e ai rinnovi, nel 2021 sono stati autorizzati 1.437 rinnovi rispetto ai trenta giorni delle autorizzazioni iniziali. La durata media, perciò, è stata di quarantaquattro giorni. I rinnovi sono diminuiti del 4% in confronto al 2020. L'intercettazione più lunga autorizzata da un giudice federale è avvenuta nel Massachussets, dove nel 2021 ne è terminata una disposta nel 2020 e rinnovata dieci volte, per un totale di 330 giorni. Più lunga ancora è stata l'intercettazione per narcotraffico autorizzata da un giudice statale a Nassau, New York, che in forza di quattordici rinnovi è durata 383 giorni.

Il costo medio di una *wiretap* nel 2021 è stato di 161.818 dollari, con un aumento del 35% per cento sul 2020.

[27] Le schede sono state tradotte ed elaborate dal Servizio Studi del Senato sulla base delle informazioni fornite sulla materia dai Parlamenti dei paesi aderenti alla rete interparlamentare ECPRD (*European Center for Parliamentary Research and Documentation*).

Albania

In **Albania** la materia è disciplinata dal Codice di procedura penale (artt. 221 e ss.) e dalla legge n. 9157 del 4.12.2003 sull'intercettazione delle comunicazioni elettroniche. Il codice penale disciplina puntualmente i limiti e i presupposti per l'utilizzo di questo mezzo di indagine. Le intercettazioni sono consentite solo nell'ambito di procedimenti per reati commessi intenzionalmente, punibili con una pena detentiva non inferiore a sette anni nel massimo; per reati dolosi, commesso con mezzi di telecomunicazione o con l'uso di tecnologie informatiche o telematiche. L'intercettazione può essere disposta nei confronti dell'indagato, di ogni persona che si ritiene riceva o trasmetta comunicazioni alla persona sospettata; di ogni persona che partecipa a transazioni con l'indagato; di ogni persona la cui sorveglianza può portare alla scoperta del luogo o dell'identità dell'indagato. Il risultato dell'intercettazione è valido nei confronti di tutte le persone coinvolte nella comunicazione.

Le operazioni captative che devono essere ritenute indispensabili per la prosecuzione delle indagini avviate e nel caso in cui esista un ragionevole dubbio sulla persona e sulla base di prove che essa abbia commesso un reato, devono essere autorizzate dal giudice, su proposta del pubblico ministero.

Nel provvedimento motivato del giudice devono essere indicate le modalità e i tempi di esecuzione, che non possono superare i quindici giorni. Tale termine può essere prorogato dal tribunale per un periodo di 15 giorni, su richiesta motivata del pubblico ministero, ogni qualvolta sia necessario e che l'esito dell'intercettazione detti la necessità di prorogare il termine.

Contro la decisione che autorizza un'intercettazione può essere presentato ricorso entro dieci giorni dalla data in cui l'interessato è venuto a conoscenza dell'intercettazione, per violazione dei limiti fissati dalla legge. Il ricorso è esaminato in camera di consiglio dalla corte d'appello. Se il ricorso è ritenuto fondato, la corte d'appello revoca la decisione che autorizza l'intercettazione e ordina la cancellazione di tutto il materiale ottenuto tramite l'intercettazione.

Le intercettazioni possono essere eseguite solo attraverso apparecchiature installate in luoghi progettati, autorizzati e controllati dal pubblico ministero. L'intercettazione e il verbale di trascrizione sono effettuati dagli ufficiali di polizia giudiziaria, sotto la direzione e la supervisione del pubblico ministero del caso.

I verbali e le registrazioni sono custoditi dall'ufficio del pubblico ministero che ha disposto l'intercettazione fino al passaggio in giudicato della decisione, ad eccezione di quelli di cui è vietato l'uso. I risultati delle intercettazioni possono essere utilizzati in altri procedimenti solo se sono indispensabili per le indagini sui reati. In questi casi, i verbali e le registrazioni dell'intercettazione devono essere depositati presso l'altra autorità procedente.

Con riguardo ai divieti di utilizzo, non possono essere utilizzate le intercettazioni di conversazioni o comunicazioni di coloro che sono obbligati a mantenere il segreto a causa della loro professione o del loro dovere, a meno che

tali persone non abbiano già testimoniato sugli stessi fatti o abbiano rivelato tali informazioni in qualsiasi altro modo. Il tribunale ordina la distruzione dei documenti delle intercettazioni di cui è vietata l'utilizzazione, salvo che costituiscano prove materiali.

Il codice di procedura penale chiarisce che le **intercettazioni preventive** sono disciplinate da una legge speciale e che i risultati di tali operazioni non possono essere utilizzati come prova. La legge n. 9157 del 4.12.2003 sull'intercettazione delle comunicazioni elettroniche stabilisce le procedure da seguire per l'intercettazione preventiva delle comunicazioni elettroniche da parte delle istituzioni statali di intelligence istituite dalla legge per l'adempimento dei propri compiti, nonché le procedure che devono essere seguite dalle persone incaricate di condurre l'intercettazione. Il Servizio di intelligence nazionale, il servizio di intelligence/servizio di intelligence di polizia del ministero responsabile per l'ordine e la sicurezza pubblica, il ministero della Difesa, il ministero delle Finanze, il ministero della Giustizia, il National Bureau of Investigation, nonché qualsiasi altro servizio di intelligence/polizia stabilito dalla legge, hanno il diritto di richiedere l'intercettazione, al fine di garantire i dati necessari per l'adempimento dei loro doveri legali. Le intercettazioni preventive devono essere esaminate entro 48 ore dalla loro richiesta ed essere autorizzate dal presidente della Corte d'appello contro la corruzione e la criminalità organizzata o, in sua assenza, dal vicepresidente. Tutte le decisioni di intercettazione di comunicazioni elettroniche sono valide per un periodo fino a tre mesi e prorogabili per ulteriori tre mesi.

Armenia

Secondo il Codice di procedura penale (artt. 26 e ss.) della Repubblica di Armenia, le intercettazioni possono essere effettuate, durante il procedimento, solo su decisione del tribunale, nei casi e secondo la procedura stabiliti dalla legge. Il controllo delle comunicazioni digitali, comprese quelle telefoniche, è un tipo di operazione investigativa segreta (articolo 241, parte 1, punto 4). Secondo l'articolo 249 (Controllo delle comunicazioni digitali, comprese quelle telefoniche) il controllo delle comunicazioni digitali, comprese quelle telefoniche, mediante l'utilizzo di mezzi tecnici speciali o di altro tipo, consiste nell'individuazione, raccolta, registrazione e archiviazione segreta dei dati di cui alla parte 2 del presente articolo da parte di persone fisiche o giuridiche che li possiedono.

2. Le comunicazioni digitali, comprese quelle telefoniche, sono soggette a controllo:

1) nel caso di una rete telefonica fissa o mobile, il contenuto della conversazione telefonica, testi, immagini, suoni, video e altri messaggi, le chiamate in entrata e in uscita dell'abbonato, l'ora di inizio e fine della comunicazione telefonica, in caso di inoltro della chiamata telefonica, il numero di telefono a cui è stata trasferita la chiamata telefonica;

2) nel caso di comunicazioni via Internet, comprese le comunicazioni telefoniche via Internet e i messaggi elettronici trasmessi via Internet, il contenuto della comunicazione, le chiamate in entrata e in uscita delle telefonate via Internet.

I dati digitali riservati archiviati sono soggetti a distruzione immediata se non vengono recuperati dall'organo investigativo entro 90 giorni dalla relativa decisione del tribunale.

Ai sensi dell'articolo 206 del Codice penale della Repubblica di Armenia (Violazione della segretezza della corrispondenza, delle conversazioni telefoniche e di altre forme di comunicazione)

1. La violazione illegale della segretezza della corrispondenza, delle conversazioni telefoniche e di altre forme di comunicazione di una persona è punita con una multa dell'importo massimo di venti volte, o con lavori pubblici per un periodo da ottanta a centocinquanta ore, o con la restrizione della libertà per un periodo massimo di due anni, o con la reclusione a breve termine per un periodo massimo di due mesi, o con la reclusione per un periodo massimo di due anni. 2. L'atto previsto nella Parte 1 del presente articolo, commesso: 1) con l'uso di poteri ufficiali o di servizio o con l'influenza ad essi condizionata; o 2) con l'uso di mezzi tecnici speciali per la raccolta di informazioni segrete, è punito con una multa da dieci a trenta volte, o con lavori pubblici da cento a duecento ore, o con la privazione del diritto di ricoprire determinate cariche o di esercitare determinate attività per un periodo massimo di cinque anni, o con la restrizione della libertà per un periodo massimo di tre anni, o con la reclusione di breve durata da uno a due mesi, o con la reclusione per un periodo massimo di tre anni.

Secondo la legge della Repubblica di Armenia sull'attività di intelligence operativa, l'articolo 9, parte 1, stabilisce che l'attuazione delle misure di intelligence operativa delle intercettazioni telefoniche previste dalla presente legge è assicurata - come prescritto dalla presente legge - solo dal dipartimento tecnico operativo generale che opera all'interno del sistema dell'Organo repubblicano di sicurezza nazionale della Repubblica d'Armenia (di seguito denominato "il dipartimento generale"), su richiesta degli organi competenti per l'attuazione di tali misure di intelligence operativa. Nell'ordinamento Armeno possono essere condotte intercettazioni durante l'attività di intelligence operativa. Ai sensi dell'articolo 32 della legge della Repubblica di Armenia sull'attività di intelligence operativa, gli organismi, compresi gli organismi di sicurezza nazionale, che hanno la competenza di attuare la misura di intelligence operativa delle intercettazioni telefoniche, per effettuare le intercettazioni telefoniche devono presentare al Dipartimento generale l'estratto della decisione del tribunale e la decisione del capo dell'organismo che effettua l'attività di intelligence operativa sull'attuazione delle misure di intelligence operativa. L'estratto è fornito dal tribunale insieme alla decisione sulla suddetta attività di intelligence operativa e contiene solo il numero di telefono oggetto di intercettazione.

Nel caso in cui il ritardo nell'attuazione delle misure di intelligence operativa possa portare a un atto di terrorismo o a eventi o azioni che minacciano la sicurezza statale, militare o ambientale della Repubblica d'Armenia, il Dipartimento generale assicura l'attuazione di tali misure; l'organismo, comunque, che ha presentato al Dipartimento generale una mozione per l'attuazione di tali misure di intelligence operativa è tenuto a presentare al Dipartimento generale, entro quarantotto ore, l'estratto della decisione del tribunale che autorizza o nega l'autorizzazione ad attuare tali misure.

In caso di mancata presentazione dell'autorizzazione del tribunale entro quarantotto ore, o in caso di presentazione al Dipartimento generale della decisione del tribunale che nega l'autorizzazione all'attuazione delle misure di intelligence operativa, tale attività deve essere immediatamente interrotta e le informazioni e i materiali già ottenuti devono essere immediatamente distrutti dall'organismo che attua la misura. Il capo dell'Organo repubblicano di sicurezza nazionale della Repubblica d'Armenia è tenuto immediatamente al Primo Ministro della Repubblica d'Armenia su ogni caso previsto dalla presente parte.

Austria

Le intercettazioni[28], quale mezzo di ricerca della prova, si distinguono in sorveglianza di comunicazioni e di persone[29], divulgazione di dati relativi alla trasmissione di messaggi e localizzazione di dispositivi tecnici[30]. Per l'Unità IV/A/4 (Special Operations Technology) esiste un solo tipo di intercettazioni, denominato "Lawful Interception" (LI), per cui i dati vengono inviati dai fornitori di servizi di comunicazione (Csp) direttamente alla "Legal Enforcement Agency" (LEA). Le condizioni procedurali per l'esercizio delle operazioni di intercettazione sono contenute nell'art. 135, comma 3, del codice di procedura penale, nonché agli articoli da 137 a 140[31]. Qualora dalle predette operazioni emergessero indizi relativi ad un reato diverso da quello per cui si procede, ove il provvedimento sia stato legittimamente disposto e autorizzato, è possibile che questi vengano utilizzati in giudizio, sempre che si tratti di reati per i quali è consentita l'intercettazione di comunicazioni[32], mentre se fosse la videosorveglianza (di cui all'art. 136 ccp.) a rivelare indizi di un reato diverso, l'utilizzabilità della misura, legittimamente disposta e autorizzata, sarebbe ammessa solo sei i risultati occorressero per provare un "crimine"[33], salvo il caso di videosorveglianza all'esterno delle abitazioni[34]. I provvedimenti di intercettazioni telefoniche e di audiovideo sorveglianza devono essere disposti dalla procura e ottenere l'approvazione del tribunale[35]. Sebbene non sia prevista una durata massima, le autorizzazioni giudiziali devono indicare il momento iniziale e finale delle

[28] Disciplinate dagli articoli da 134 a 140 del codice di procedura penale austriaco (ccp.).

[29] La "sorveglianza delle comunicazioni" consiste in un controllo delle comunicazioni e delle informazioni inviate, trasmesse o ricevute da una persona attraverso una rete di comunicazione o un servizio della società dell'informazione (art.134, comma 3, ccp.). La "sorveglianza di persone" si sostanza in un audiovideo sorveglianza di un individuo, a sua insaputa, per il monitoraggio della sua condotta e delle sue dichiarazioni e conversazioni riservate, mediante l'utilizzo di apparecchiature tecniche per la trasmissione o registrazione audiovideo (art.134, comma 4, ccp.).

[30] Art.134, comma 2, ccp.

[31] In particolare, le limitazioni sono poste a tutela del diritto di rifiutarsi di testimoniare, soprattutto in relazione alla riservatezza che connota il rapporto avvocato-cliente, o del segreto editoriale.

[32] Pertanto, le prove potranno essere utilizzate in caso di reato commesso intenzionalmente e punito con la pena della reclusione superiore a un anno e nel caso di sequestro di persona (art. 135, co. 2, lett. 1, ccp.). Le operazioni di spionaggio sono consentite solo al fine di contrastare crimini gravi per i quali è prevista una pena detentiva superiore a dieci anni, fenomeni di criminalità organizzata e terrorismo. Il rispetto della privacy e della riservatezza, pur nei limiti in cui tali misure possono derogarvi, è garantito attraverso strumenti diversi, tra cui, ad esempio, le disposizioni del codice penale, la disciplina giudiziaria delle informazioni classificate, il regolamento interno di polizia per il trattamento delle informazioni classificate.

[33] Secondo l'art. 17 del codice di procedura penale, un crimine è un reato (grave) intenzionale punibile con la reclusione a vita o con la reclusione superiore a tre anni.

[34] L'ammissibilità, difatti, non dipende da uno specifico provvedimento e può pertanto essere utilizzata per provare qualsiasi reato.

[35] Salvo il caso di rapimento, ai sensi dell'art. 136, comma 1, lettera 1, ccp., in cui la sorveglianza può essere condotta in modo indipendente dall'autorità giudiziaria che dirige le indagini. L'"ingresso nei luoghi", invece, richiede una specifica approvazione del tribunale.

operazioni di sorveglianza[36], mentre per quanto riguarda le "Lawful Interception" non esiste una durata standardizzata. I dati ricavati dalle intercettazioni vengono inseriti nell'archivio online gestito da BMI IV/A/4 e, una volta chiuso il caso, vengono archiviati su un supporto esterno (CD/DVD/BD) presso il Ministero Federale della Giustizia. La diffusione di filmati, registrazioni o qualunque altro materiale ottenuto mediante intercettazioni, ove non risulti rilevante per il procedimento giudiziario, è punita ai sensi dell'articolo 30, comma 3, del codice penale[37]. Le registrazioni ritenute necessarie ai fini della prova vengono inizialmente selezionate dalle autorità investigative penali e, se necessario, anche dalla procura e dai tribunali[38]. Il rimborso dei costi sostenuti dai fornitori per le operazioni di intercettazione delle comunicazioni (art. 135, commi 2 e 3, ccp.) è disciplinato da un'apposita ordinanza concernente le relative tariffe[39].

[36] Ai sensi dell'art. 138, comma 1, numero 4, ccp.. Secondo il principio generale stabilito dall'art. 5 del codice, inoltre, le autorità investigative penali, le autorità giudiziarie e i tribunali devono scegliere la misura che meno leda i diritti della persona interessata.

[37] A seconda delle circostanze del caso concreto, tale comportamento potrebbe anche rilevare come trattamento dei dati a scopo di lucro o danno, ai sensi dell'articolo 63 della legge sulla protezione dei dati.

[38] Ai sensi dell'articolo 139, comma 1, ccp., all'imputato deve essere data la possibilità di visionare e ascoltare tutti i risultati (articolo 134, comma 5, ccp.), pur potendo l'autorità giudiziaria, su richiesta di terzi interessati, escludere i risultati non rilevanti ai fini del procedimento. I risultati ottenuti tramite i provvedimenti investigativi che non presentino alcuna rilevanza ai fini della prova in giudizio o che non risultino altrimenti rilevanti o attinenti al procedimento, su richiesta dell'imputato o anche d'ufficio, devono essere distrutti. La presa in consegna di un computer e la registrazione dello schermo non rientrano tra le misure previste dal codice di procedura penale.

[39] I relativi costi sono elencati nell'ÜKVO (ordinanza sui costi di monitoraggio) RIS - Ordinanza sui costi di monitoraggio - Testo unico federale, versione del 24.02.2023 (bka.gv.at).

Belgio

Le intercettazioni possono costituire mezzi di ricerca della prova ove il tribunale ritenga opportuno che l'"intercettazione" in senso lato di una telecomunicazione possa essere utilizzata come prova in giudizio senza violare una ragionevole aspettativa di privacy del soggetto interessato. La legge 30 giugno 1994, difatti, reca il principio generale per cui è fatto divieto di intercettare comunicazioni private durante la loro trasmissione, sanzionandone la violazione con la pena della reclusione, oltre a sanzioni pecuniarie. In deroga, vengono previste due ipotesi del codice investigativo penale: l'articolo 88-*bis*, che consente a determinate condizioni la localizzazione e la rilevazione di dati relativi a una comunicazione privata; gli articoli da 90-*ter* a 90-*decies*, che contengono la disciplina circa l'intercettazione e la registrazione di telecomunicazioni. I presupposti per l'autorizzazione, concessa dal giudice istruttore su istanza del pubblico ministero, sono particolarmente stringenti nel caso di intercettazione e registrazione di conversazioni, dovendo sussistere, in un contesto eccezionale, gravi indizi circa la commissione di uno dei reati specificamente previsti[40]. Spetta poi agli agenti di polizia (squadre specializzate) procedere all'esecuzione mediante l'intervento dell'operatore delle telecomunicazioni. La durata delle operazioni viene stabilita dal giudice istruttore, dovendo in ogni caso rispettare il limite massimo di due mesi (rilevazione/localizzazione) o un mese dalla data del provvedimento che dispone la misura di sorveglianza (intercettazione/registrazione)[41]. Della comunicazione intercettata viene steso un verbale, oltre alla eventuale traduzione, e, unitamente alla registrazione, vengono conservate in apposito registro presso la cancelleria del tribunale[42]. La captazione informatica è consentita senza particolari vincoli[43]. Non sono consentite intercettazioni esplorative o con finalità preventive, sebbene le prove eventualmente acquisite in ordine ad un reato diverso da quello per cui le intercettazioni telefoniche furono disposte potranno essere legittimamente impiegate anche in procedimenti penali diversi. Il costo delle intercettazioni nel 2017, a seguito di un accordo con gli operatori delle telecomunicazioni, è stato ridotto 6 milioni di euro, a fronte dei 13/14 milioni di euro degli anni precedenti.

[40] Fermo il rispetto dei principi di proporzionalità e sussidiarietà. Nel caso di flagranza di reato, il pubblico ministero può provvedere egli stesso se si tratta di uno dei reati per i quali l'adozione della misura è prevista. Inoltre, è il giudice istruttore a dover indicare le circostanze di fatto che giustificano l'adozione del provvedimento di localizzazione/rilevazione nei confronti del sospettato, in relazione alla frequenza nell'utilizzo dei mezzi di comunicazione o all'abitualità con cui viene frequentato un determinato ambiente.

[41] È possibile una proroga, per un nuovo periodo non superiore a un mese, per un massimo di sei mesi.

[42] Le conversazioni, comunicazioni o telecomunicazioni soggette al segreto professionale non devono essere messe a verbale e saranno depositate in un file sigillato. Delle intercettazioni telefoniche devono essere trascritti solo i passaggi rilevanti per l'indagine. Indipendentemente dalla selezione operata dagli agenti di polizia giudiziaria, il giudice istruttore può valutare quali parti delle comunicazioni registrate siano rilevanti ai fini dell'indagine e chiederne la trascrizione. La difesa deve sempre poter consultare il materiale risultante dall'intercettazione.

[43] Fatta eccezione per le fattispecie delittuose di frodi informatiche.

Bulgaria

Si definiscono intercettazioni o mezzi speciali di intelligence (SIM) i mezzi tecnici e i metodi operativi impiegati per rinvenire prove materiali[44] e per la prevenzione e l'accertamento di reati dolosi gravi, specificatamente previsti dal codice penale[45]. Le intercettazioni, a seconda della metodologia di captazione, si distinguono in intercettazioni in tempo reale (modalità interattiva) e registrazioni di conversazioni (modalità passiva)[46]. In tempi più recenti è invalso altresì l'utilizzo di dispositivi di intercettazione interattivi con schede GSM, in grado di trasmettere il segnale audio non appena il suono raggiunga il microfono[47]. Il ricorso ai mezzi speciali deve essere sempre autorizzato dal presidente del tribunale distrettuale, giacché solo l'Agenzia statale per la sicurezza nazionale (SANS) e l'Agenzia statale per le operazioni tecniche (SATO) possono utilizzare tali strumenti con finalità di prevenzione rispetto alla commissione di gravi reati. Qualsiasi forma di captazione occulta di una conversazione costituisce un reato in assenza dei presupposti specificamente previsti dalla legge speciale. Difatti, è il procuratore capo a dover presentare al giudice un'istanza scritta e motivata ai fini del loro impiego nel procedimento istruttorio[48]. La durata delle operazioni è di venti giorni nei casi di cui all'art. 12, comma 1, numero 4, e due anni nei casi di prevenzione di reati dolosi gravi, di cui al capo primo della parte speciale del codice penale. Le registrazioni avvengono secondo il procedimento previsto dal codice di procedura penale[49]. Le attività di intercettazione sono svolte dall'Agenzia

[44] Intendendosi, ad esempio, registrazioni su pellicola, registrazioni audio/video, fotografie e altri oggetti ai sensi della legge sui mezzi speciali di intelligence (SIMA).

[45] Ai sensi dell'art. 3, comma 1, della legge sui mezzi speciali di intelligence (SIMA). L'intercettazione con finalità preventive può essere utilizzata solo ed esclusivamente in presenza di espresso consenso scritto di una persona la cui vita o la cui salute sia minacciata o da chi abbia acquisito la qualità di testimone in un procedimento penale (art. 12, comma 3). Ai sensi dell'art. 12, comma 2, le intercettazioni vengono altresì impiegate come strumento atto a proteggere la vita o la proprietà di una persona che abbia dato espresso consenso all'utilizzo di tale metodo.

[46] È possibile combinare insieme queste due tipologie di intercettazioni. Ciascuna delle due categorie è inoltre suddivisa in base al tipo di attivazione del dispositivo: attivazione manuale (pressione di un pulsante), attivazione vocale e attivazione tramite movimento.

[47] Sistema ottimale, sebbene funzioni in tempo reale, per intercettare un soggetto che si trovi distante o quando l'accesso ai luoghi privati venga concesso raramente.

[48] Una serie di autorità (Direzione Principale "Polizia di Stato", Direzione Principale "Lotta alla Criminalità Organizzata", Direzione Principale "Polizia di Frontiera", Direzione "Sicurezza Interna", Direzioni Regionali del Ministero dell'Interno, Direzioni Specializzate, ad eccezione della Direzione "Operazioni Tecniche", direzioni territoriali e dipartimenti territoriali indipendenti della National Security State Agency) possono richiedere tali misure. I capi degli organi e, per la direzione, il presidente della Commissione per il Contrasto alla Corruzione e per la Confisca dei Beni Acquisiti Illegalmente presentano la richiesta ai presidenti del tribunale della città di Sofia, ai tribunali distrettuali o militari competenti o a un vicepresidente da questi autorizzati. Nei casi di competenza della Procura europea, ai sensi del regolamento (UE) 2017/1939, del 12 ottobre 2017, che istituisce una cooperazione rafforzata per l'istituzione di una Procura europea (GU L 283/1 del 31 ottobre 2017), la richiesta scritta e motivata deve essere presentata al tribunale dal procuratore europeo o da un procuratore europeo delegato.

[49] Entro 24 ore dalla loro redazione, una copia delle prove e il supporto di registrazione devono essere inviati, sigillati, all'autorità competente. Entro un mese dal termine delle operazioni di intelligence,

statale “Operazioni Tecniche” e dalla Direzione “Operazioni Tecniche” dell'Agenzia statale “Sicurezza Nazionale”[50]. Tutte le informazioni ottenute, anche se irrilevanti ai fini del procedimento giudiziario, dovranno essere classificate come segrete o “top secret”[51]. L’autorità richiedente è incaricata di selezionare il materiale ai fini della prova a sostegno dell'accusa o dell’imputato. Secondo quanto previsto dalla legge sui mezzi speciali di intelligence, la captazione mediante computer non è uno strumento per raccogliere informazioni, ma rientra nell'ipotesi di sorveglianza. Le informazioni acquisite in relazione ad un determinato procedimento non possono essere utilizzate come mezzi di prova in ordine ad un reato diverso. La gestione dei costi sostenuti dall'Agenzia di Stato “Operazioni Tecniche” rientra nelle prerogative della stessa Agenzia[52].

l'organo competente presenta una relazione al giudice recante i dati sul tipo di operazione, sulla sua durata e sulle prove raccolte o distrutte. L'Ufficio Nazionale svolge attività rilevanti in relazione alla regolarità della tenuta dei registri presso gli enti e le strutture, nonché per la conservazione e la distruzione delle informazioni acquisite attraverso di essi.

50 La garanzia della integrità e della riservatezza delle informazioni è assicurata dalla legge sulla Tutela delle Informazioni Classificate, dalle disposizioni del codice penale e dalla legge sui mezzi speciali di intelligence.

51 Pertanto, la loro diffusione è vietata e si incorre in responsabilità penale in caso di inosservanza. È responsabile di un reato d’ufficio chi abbia diffuso registrazioni o materiale comunque ottenuto mediante le intercettazioni ai sensi dell'articolo 284-*quinquies* cp.

52 Sono collocati nella sezione "Bilancio", votata dall'Assemblea nazionale della Repubblica di Bulgaria.

Canada

Le intercettazioni sono un mezzo di ricerca della prova, come previsto dalla relazione annuale 2020 sull'uso della sorveglianza elettronica (che ne disciplina condizioni, modalità d'uso e ogni altro aspetto) e dalle disposizioni contenute nella parte VI del codice penale[53]. Nello specifico, l'articolo 184, comma 1, del codice, configura come reato l'intercettazione di una comunicazione privata mediante qualsiasi dispositivo elettromagnetico, acustico, meccanico o di altro tipo, e tuttavia, ai fini delle indagini penali, è prevista un'eccezione. A tal proposito, possono distinguersi cinque tipologie di "sorveglianza": audio (art. 185 del Codice); video (art. 487, comma 1, del Codice); rinnovi (art. 186 del Codice); audio di emergenza (art. 188 del Codice) e video di emergenza (art. 487, comma 1, del Codice)[54]. Solo gli ufficiali e gli agenti designati possono richiedere e ottenere l'autorizzazione giudiziaria[55] ad intercettare comunicazioni private e solo per alcuni reati gravi elencati all'art.183 del codice penale. Le autorizzazioni non sono rilasciate per un periodo superiore a 60 giorni (art. 186, comma 4, lettera e), sebbene sia possibile, a determinate condizioni, chiedere un rinnovo che ne prolunghi la durata (art. 186, comma 6 e 7). Per quanto concerne, invece, le intercettazioni di "emergenza", l'autorizzazione può essere rilasciata per un periodo di trentasei ore alle condizioni poste dal giudice (art. 188). L'articolo 187 del codice penale stabilisce che i documenti ricavati dalle intercettazioni sono riservati e devono essere conservati in un plico sigillato e custoditi dal tribunale. Alla luce delle linee guida per gli agenti e gli ufficiali di pace designati dal Ministro della Pubblica Sicurezza canadese (PS), le informazioni ricavate da comunicazioni intercettate possono essere impiegate come materiale probatorio solo se all'imputato sia stata comunicata con ragionevole preavviso l'intenzione di impiegarle come prova in giudizio[56]. La divulgazione di informazioni acquisite mediante intercettazione, ai sensi dell'art. 193, comma 1, del codice penale, costituisce reato. Il codice penale include disposizioni per le intercettazioni preventive autorizzate, finalizzate a prevenire lesioni personali, e non autorizzate, volte a prevenire danni imminenti a persone o proprietà, di cui all'art. 184, comma 1, n. 1, e comma 4.

[53] Legge federale che contiene disposizioni sulla maggior parte dei reati e delle relative procedure.

[54] Tabella 1 della relazione annuale 2020 sull'uso della sorveglianza elettronica.

[55] Fermi i principi di sussidiarietà e proporzionalità e le altre condizioni che il giudice dovrà verificare a norma della relazione annuale 2020 sull'uso della sorveglianza elettronica.

[56] La comunicazione deve essere accompagnata dalla trascrizione della registrazione, che specifichi la data, l'ora e il luogo della conversazione (art. 189, commi 5 e 6, codice penale).

Croazia

Ove sussista un fondato sospetto circa la commissione da parte dell'indagato/imputato di un reato per il quale è prevista la pena pecuniaria o la reclusione fino a cinque anni, il procuratore di Stato può provvedere egli stesso o ordinare all'investigatore di intraprendere iniziative finalizzate alla raccolta di prove da utilizzare in giudizio. Il procuratore deve, in primo luogo, notiziare il soggetto interessato attraverso la consegna dell'avviso di svolgimento delle azioni investigative, entro tre giorni dal loro inizio. L'autorità che conduce la ricerca può decidere di segretarla in tutto o in parte qualora ritenga che un'eventuale divulgazione di informazioni finirebbe per pregiudicarne l'esito. Chiunque venga a conoscenza del contenuto degli atti compiuti durante lo svolgimento dell'indagine segreta è tenuto a mantenere segreti i fatti o le informazioni appresi in tale occasione. La disciplina delle intercettazioni è contenuta nella legge sulla procedura penale (NN 152/08, 76/09, 80/11, 121/11, 91/12, 143/12, 56/13, 145/13, 152/14, 70/17, 126/19, 126/19, 130/20, 80/22). Ove l'istruttoria non potesse essere altrimenti svolta o rischiasse di divenire eccessivamente difficoltosa, il giudice istruttore, su richiesta scritta e motivata del procuratore di Stato, può ordinare, nei confronti della persona sospettata di aver commesso o di aver partecipato alla commissione di uno dei reati di cui all'articolo 334 della legge sulla procedura penale, l'adozione di misure che limitino temporaneamente alcuni diritti costituzionali. Tra questi provvedimenti, eseguiti dalla polizia, vi rientrano: la sorveglianza e l'intercettazione di conversazioni telefoniche e mediante altri mezzi di comunicazione a distanza; l'intercettazione, la raccolta e la registrazione di dati informatici; l'ingresso e la registrazione nei locali ai fini di sorveglianza; il pedinamento e la registrazione di persone e oggetti; l'utilizzo di investigatori e informatori sotto copertura[57]. In generale, le iniziative volte alla raccolta delle prove possono avere una durata massima di tre mesi, sebbene, su proposta del procuratore, il giudice istruttore abbia la facoltà di concedere una proroga di altri tre mesi ove lo ritenga necessario[58]. Nell'evenienza in cui i presupposti di cui all'articolo 332, comma 1, della legge dovessero venir meno, il giudice istruttore è tenuto a disporre la sospensione delle azioni[59]. La divulgazione di informazioni concernenti le indagini, in quanto coperte da segreto, costituisce reato. Se nel corso delle operazioni venissero registrati dati e informazioni relativi ad altro autore o reato (pur sempre appartenente al novero dei delitti per i quali le intercettazioni possono essere disposte), è necessario inviare il materiale alla procura, potendo essere eventualmente utilizzato come prova in altro procedimento penale[60].

[57] Art. 332, comma 1, della legge sulla procedura penale.

[58] Disposizioni più specifiche sono contenute nell'art. 334 della legge sulla procedura penale, in particolare, sui casi in cui è possibile che venga concessa una proroga di altri sei mesi.

[59] Se la Procura rinuncia all'azione penale o se i dati e le informazioni ricavati non sono necessari per il procedimento, il materiale raccolto deve essere distrutto sotto la vigilanza del giudice istruttore.

[60] Art. 335, comma 6, della legge sulla procedura penale.

Estonia

In Estonia le intercettazioni sono un mezzo di ricerca della prova e possono essere utilizzate sia per fini di giustizia che come strumento di prevenzione del crimine. La disciplina è recata dal Codice di procedura penale[61]. L'intercettazione è autorizzata dal gip per un periodo non superiore a due mesi, prorogabile ogni volta fino a due mesi, per massimo un anno. Solo le agenzie governative possono effettuare intercettazioni (es. Polizia, Guardie di frontiera, Servizio di sicurezza interna, Imposte e dogane, Polizia militare) al fine di: raccogliere informazioni a scopo preventivo; eseguire un ordine per latitanza; raccogliere informazioni nell'ambito di un procedimento di confisca e/o penale. In Estonia è operativo il Sistema informativo nazionale di sorveglianza, *database* del sistema informativo statale per il trattamento dei relativi dati. Le operazioni segrete devono rispettare determinati principi: in generale, non possono mettere in pericolo la vita o la salute di una persona, creare rischi ingiustificati per la proprietà e l'ambiente o interferire immotivatamente con altri diritti personali. Le informazioni raccolte costituiscono prova, a condizione che siano stati rispettati i requisiti di legge al momento della richiesta di autorizzazione, della relativa concessione e dello svolgimento dell'operazione. Dell'attività di sorveglianza deve essere redatto rapporto da parte dell'autorità procedente. I dati raccolti sono archiviati secondo una procedura stabilita dal Governo, su proposta del Ministro competente, tramite regolamento riservato. Le informazioni raccolte sono conservate presso l'autorità di sorveglianza e archiviate nel fascicolo penale laddove utili al giudizio. I dati raccolti in via preventiva sono conservati fino a quando non cessa la necessità di utilizzare le informazioni ivi contenute, ma non oltre 50 anni; i dati raccolti per fini di giustizia, fino alla cancellazione dal casellario giudiziale o alla prescrizione del reato. I dati ottenuti da un'operazione di sorveglianza possono essere utilizzati in altra operazione di sorveglianza, altra indagine penale, in controlli di sicurezza e, nei casi previsti dalla legge, per prevenire il riciclaggio di denaro e il finanziamento del terrorismo[62]. I dati possono essere conservati anche per scopi didattici e di ricerca. La riservatezza delle attività di intercettazione viene garantita tramite applicazione della disciplina del segreto di Stato. La diffusione di materiali acquisiti tramite intercettazioni e non rilevanti ai fini processuali è punita con una pena pecuniaria o la reclusione fino a 5 anni.

[61] Capitolo 3^1 del Codice di procedura penale estone: https://www.riigiteataja.ee/en/eli/527122021006/consolide

[62] Oltre che per verificare la conformità di una persona ai requisiti di legge quando si decide sull'impiego o sul servizio di una persona e sulla concessione di un permesso o di una licenza.

Finlandia

In Finlandia le intercettazioni sono un mezzo di ricerca della prova[63]; sono previste sia quelle a fini di giustizia, che quelle volte alla prevenzione del crimine[64]. Nella Legge sulle misure coercitive, l'intercettazione delle tlc si riferisce al monitoraggio, registrazione e altre elaborazioni di un messaggio inviato o trasmesso da un indirizzo di rete o da un dispositivo terminale attraverso una rete di comunicazione pubblica, o una rete di comunicazione collegata, al fine di determinare il contenuto del messaggio e i dati identificativi connessi. L'autorità investigativa penale può ottenere l'autorizzazione all'intercettazione di comunicazioni provenienti o destinate a una persona solo quando questa è sospettata di aver commesso un reato aggravato di cui alla Legge sulle misure coercitive (l'elenco comprende tutti i reati, tranne quelli minori). Le informazioni ottenute possono essere utilizzate nei procedimenti relativi al reato per cui si procede, mentre i dati raccolti ma non collegati al reato o collegati a un reato diverso da quello per il quale vi è stata autorizzazione, possono essere utilizzate solo a determinate condizioni[65]. Il tribunale decide sull'uso come prova delle cd. 'informazioni in eccesso'. La misura, della durata massima di un mese, rinnovabile, è autorizzata dai tribunali distrettuali e in genere eseguita dalla polizia. In casi urgenti, il funzionario autorizzato all'arresto può decidere la misura sino a quando il tribunale non si pronuncia sulla richiesta di autorizzazione. I dati sono conservato in un sistema informatico sicuro per il solo tempo necessario. La riservatezza è garantita dalla confidenzialità e dal numero ridotto di addetti, agenti sotto la responsabilità di un unico funzionario, responsabile, eventualmente, del reato di abuso di ufficio (punibile con multa o reclusione fino a 2 anni). Il materiale non rilevante non deve essere conservato più a lungo del necessario, indi distrutto. Le registrazioni possono essere esaminate dal tribunale, da un funzionario con potere di arresto e dall'investigatore del reato oggetto di indagine e se del caso, su ordine di questi, da esperti. È consentito l'uso del captatore informatico[66]. L'ambito di applicazione delle misure preventive riguarda reati potenzialmente lesivi della sovranità, incitanti alla guerra; includono tradimento, spionaggio, divulgazione di segreto nazionale, intelligence illegale, terrorismo, ovvero - rispetto alle dogane e al controllo delle frontiere, reati rilevanti (es. droga, ingresso illegale, traffico di esseri umani).

63 Alle condizioni stabilite dal Coercive Measures Act (806/2011), ch. 10 section 3 (p. 54).

64 Le intercettazioni in ambito penale sono regolate dal Coercive Measures Act (806/2011), ch. 10 (p. 54–); quelle preventive sono disciplinate da: Police Act (872/2011), ch. 5 (p. 14–), Act on Crime Prevention by Customs (623/2015, in finlandese), ch. 3, Act on Crime Prevention by the Border Guard (108/2018), chs 3–4 (p. 7–).

65 ch. 10 section 56 of the Act (p. 86).

66 Coercive Measures Act (806/2011), ch. 8 sections 20–29 (p. 46–).

Georgia

In Georgia le intercettazioni, sia a fini di giustizia che a scopo preventivo, costituiscono un mezzo di ricerca della prova e sono disciplinate dal Codice di Procedura Penale e da altre fonti[67]. Il c.p.p. prevede i seguenti atti investigativi, svolgibili anche contemporaneamente: intercettazione e registrazione occulta di comunicazioni telefoniche; recupero e registrazione di informazioni da un canale di comunicazione (tramite collegamento a strutture e/o linee di comunicazione, reti informatiche e dispositivi), sistemi informatici (sia direttamente che a distanza) e installazione del relativo *software* nel sistema informatico; geolocalizzazione; monitoraggio di trasferimenti postali e telegrafici (eccetto posta diplomatica); video/audio/foto registrazione; sorveglianza elettronica con mezzi tecnici il cui uso non arrechi danno alla vita umana, alla salute e all'ambiente. La Legge sulle attività di controspionaggio prevede speciali misure tecniche[68] finalizzate a ottenere informazioni sulle attività di intelligence e/o terroristiche di servizi speciali, organizzazioni e gruppi. Le intercettazioni sono effettuate dall'Agenzia tecnico-operativa della Georgia, nell'ambito del Servizio di sicurezza dello Stato. Le misure sono impiegate solo in indagini penali o per garantire la sicurezza nazionale o pubblica, prevenire sommosse o reati, proteggere gli interessi economici del paese e i diritti e le libertà delle persone. È necessaria l'autorizzazione del giudice (su istanza motivata del PM) che definisce il tempo necessario al raggiungimento dell'obiettivo di indagine. Vi sono 3 fasi, in ciascuna delle quali la misura viene autorizzata per non oltre 90 giorni; se al termine l'obiettivo non è stato raggiunto, è possibile la proroga a determinate condizioni. Il materiale allegato come prova in giudizio è conservato presso il tribunale per la relativa durata e al termine deve essere distrutto; il materiale dichiarato inammissibile deve essere distrutto 6 mesi dopo la sentenza definitiva. Fino alla distruzione, i materiali sono conservati in un deposito speciale del tribunale e sono inaccessibili, ad eccezione delle parti del processo. I materiali raccolti per attività preventive sono distrutti dopo 6 mesi dalla fine dell'attività investigativa e per la tenuta è responsabile la citata Agenzia. La riservatezza è garantita tramite il Servizio per la protezione dei dati personali ed è punita la diffusione di materiali acquisiti con intercettazioni non rilevanti ai fini processuali.

---

67 Costituzione, C.p.p. Cap. XVI1, *Covert Investigative Actions*, Legge sulle comunicazioni elettroniche, Legge sulla protezione dei dati personali, Legge sulle attività di controspionaggio, Legge sulle attività operative e investigative.

68 Video e audio registrazione sotto copertura; riprese e fotografie di nascosto; uso di telecamere e altri tipi di apparecchiature elettroniche; sorveglianza elettronica; controllo della corrispondenza.

Grecia

In Grecia la disciplina che regola la procedura di intercettazione legale delle comunicazioni è recata dalla Legge n. 5002 del 2022 e dal Decreto presidenziale n. 47 del 2005. In base all'articolo 6 della citata legge, l'intercettazione delle comunicazioni per l'individuazione di reati è consentita per alcuni reati e crimini elencati nel Codice penale, nel Codice penale militare e in altre leggi correlate. La decisione di revocare la riservatezza può essere assunta solo dal competente consiglio giudiziario, su proposta del Pubblico Ministero e, in casi di emergenza, dal Procuratore o dal giudice istruttore, che deve sottoporre la questione al consiglio giudiziario. La decisione o l'ordine devono includere l'autorità richiedente, l'atto criminale e le circostanze del reato. Se non viene emessa una decisione del consiglio giudiziario entro un tempo ragionevole, i materiali non sono utilizzabili.

L'articolo 7 della Legge 5002/2022 disciplina la gestione del materiale rilevante. Si prevede che le prove sequestrate o confiscate e registrate durante la revoca del segreto possono essere allegate al relativo fascicolo solo se costituiscono una prova per l'azione penale o l'assoluzione dell'imputato, e il pubblico ministero o il magistrato inquirente è tenuto a limitare il materiale registrato a ciò che è considerato prova per l'indagine. Qualsiasi prova o conoscenza ottenuta durante l'intercettazione legale può essere utilizzata nello stesso procedimento penale, se riguarda un reato compreso nell'elenco di cui all'articolo 6. Se il consiglio giudiziario lo consente, è possibile utilizzarle in un altro processo penale, sempre per il perseguimento dei reati per i quali è prevista la possibilità di effettuare intercettazioni. In caso di atti criminali compiuti da persone in possesso di informazioni privilegiate e di manipolazioni criminali del mercato, il materiale può essere utilizzato anche in procedimenti amministrativi per l'accertamento di violazioni e l'irrogazione di multe, previa richiesta e approvazione delle autorità competenti. Le prove e il materiale devono essere distrutti tempestivamente dopo una decisione irrevocabile o una sentenza di assoluzione o se non è stato avviato un procedimento penale. L'articolo 8 della Legge 5002/2022 delinea la procedura per le intercettazioni legali. Si prevede la consegna di un estratto dell'ordinanza o della sentenza alle parti interessate e all'Autorità ellenica per la sicurezza delle comunicazioni e la privacy (ADAE), nonché la creazione di piattaforme elettroniche per eliminare la riservatezza per motivi di sicurezza nazionale. La durata dell'intercettazione legale è limitata a dieci mesi e dopo l'esecuzione dell'ordine devono essere presentate relazioni sull'attività svolta. La disposizione vieta l'uso delle informazioni ottenute tramite intercettazione legale in altri procedimenti, imponendo pene per il mancato rispetto della procedura, e prevede la digitalizzazione dei documenti archiviati relativi all'intercettazione.

Irlanda

In Irlanda le intercettazioni sono un mezzo di ricerca della prova e la relativa disciplina è recata da diverse fonti normative[69]. La legge sui servizi postali e di tlc vieta in via generale l'intercettazione di chiamate telefoniche, qualificando tale attività come reato in assenza della prescritta autorizzazione. Sono previste sia le intercettazioni per fini di giustizia, che quelle a scopo preventivo. La sorveglianza tramite dispositivo (comprendente monitoraggio, osservazione, ascolto o registrazione di una persona o gruppo di persone e/o dei loro movimenti, attività e comunicazioni, nonché di luoghi o cose) richiede una preventiva autorizzazione giudiziaria; l'intercettazione del contenuto di comunicazioni (es., telefoniche) richiede l'autorizzazione del Ministro della Giustizia, mentre l'uso di dispositivi di localizzazione e l'accesso ai dati delle comunicazioni conservati avvengono sulla base di un'approvazione interna della Polizia irlandese, della Forza di Difesa Permanente, dei Commissari delle Entrate, della Commissione per la Concorrenza e la Protezione dei Consumatori. L'autorizzazione è efficace per un periodo non superiore a 3 mesi, estendibile per un ulteriore periodo non superiore a 3 mesi; in caso di eccezionale urgenza, l'autorizzazione può essere accordata oralmente dal Ministro e poi confermata, ovvero, per i casi di autorizzazione giudiziaria, se la misura è stata approvata da un funzionario superiore, si può applicare per massimo 72 ore, oltre le quali è necessaria l'autorizzazione. L'intercettazione a fini di indagine penale è consentita per reati gravi, indagini condotte dalla Polizia irlandese o da altra autorità pubblica e se vi è la ragionevole prospettiva che la misura è utile a produrre informazioni/prove, ovvero a prevenire reati punibili con l'arresto. L'intercettazione a fini preventivi è consentita se vi è motivo di ritenere che siano in atto o in progetto attività che mettono in pericolo la sicurezza dello Stato. Ai fini delle indagini, pc e cellulari possono costituire prova, quindi essere soggetti alla misura. Vi sono restrizioni in merito alla divulgazione dell'esistenza, dell'autorizzazione e del contenuto delle comunicazioni intercettate; le domande di autorizzazione e i documenti correlati devono essere conservati per 3 anni dalla cessazione o dal giorno in cui non sono più necessari per un'azione legale o ricorso. Gli stessi termini si applicano ai materiali risultato di sorveglianza/tracciamento. I documenti sono distrutti quando non è più necessario conservarli, a meno che il Ministro non ne autorizzi la conservazione. Il Ministro competente garantisce che il materiale sia archiviato in modo sicuro, potendovi accedere solo gli autorizzati; ne viene punita la divulgazione illecita.

[69] Postal and Telecommunications Services Act 1983, Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993, Criminal Justice (Surveillance) Act 2009 and the Communications (Retention of Data) Act 2011

Lettonia

In Lettonia la materia è regolata dal Codice di procedura penale e dalla Legge sulle attività operative. Il controllo dei telefoni e di altri mezzi di comunicazione all'insaputa dei membri di una conversazione, del mittente e del destinatario, viene effettuato sulla base di una decisione del giudice istruttore, se vi è motivo di ritenere che solo in tal modo possano essere acquisite informazioni relative a reati da accertare. Ogni istituzione investigativa pubblica (Polizia di Stato, militare, fiscale e doganale, Servizio di Sicurezza dello Stato, ecc.) può avviare il controllo dei mezzi di comunicazione in relazione a un procedimento penale di propria competenza, per reati meno gravi, gravi e particolarmente gravi. La legge sulle attività operative prevede che, quando l'organo investigativo dispone di informazioni sulla preparazione di un reato o su una minaccia alla sicurezza nazionale o pubblica, vi sia una persona sospettata, accusata o condannata di aver commesso un reato, sia consentita l'applicazione di speciali misure. Queste contemplano, tra l'altro: la sorveglianza, il monitoraggio della corrispondenza (postale, telegrafica e di altro tipo, es. elettronica), l'acquisizione di informazioni espresse o memorizzate tramite mezzi tecnici, l'intercettazione di conversazioni (tramite telefono, mezzi di comunicazione elettronica e di altro tipo), la videosorveglianza di luogo non accessibile al pubblico. Nell'ambito di tali misure, possono essere effettuate registrazioni con apparecchiature video/audio, foto/cinematografiche e possono essere utilizzati sistemi informatici e mezzi tecnici, chimici e biologici, in modo però da non causare danni alla salute o all'ambiente. L'esecuzione delle attività operative avviene secondo il metodo generale o speciale: si segue il primo quando l'esecuzione non viola in modo significativo i diritti fondamentali delle persone (in tal caso, sono avviate da un funzionario con l'approvazione del suo diretto superiore o del vice-direttore); si segue, invece, il metodo speciale per l'esecuzione di misure comportanti significative violazioni dei diritti fondamentali. In tal caso occorre l'approvazione del Presidente della Corte Suprema o di un giudice della Corte da questi autorizzato, ovvero del PM. Le citate misure operative (monitoraggio della corrispondenza, ecc.), nonché il monitoraggio delle transazioni bancarie e finanziarie, l'ingresso investigativo e la sorveglianza prolungata (tracciamento) seguono sempre il metodo speciale. L'autorizzazione è accordata per massimo tre mesi, prorogabile in caso di necessità giustificata per un periodo massimo di ulteriori tre mesi. Il numero di volte in cui è possibile prorogare l'autorizzazione non è limitato, tuttavia l'esecuzione delle misure delle attività operative pertinenti è consentita solo durante lo svolgimento del processo investigativo. Ove sia necessaria un'azione immediata per scongiurare o individuare atti di terrorismo e reati gravi (es. omicidio, disordini) e qualora siano in pericolo la vita, la salute o i beni delle persone, le misure possono essere eseguite con approvazione del PM. L'approvazione di un giudice deve essere ottenuta il giorno lavorativo successivo, non oltre le 72 ore. Il controllo di conformità alla legge delle attività operative è

effettuato dal Procuratore generale o da procuratori da questi autorizzati. Qualora si ritenga che, nello svolgimento delle citate attività, l'organo procedente abbia violato i diritti e le libertà della persona, questa ha il diritto di presentare un reclamo al PM che, dopo aver condotto un esame, fornirà un parere sulla conformità delle azioni in esame, fermo restando il diritto di agire in giudizio.

Lituania

In Lituania le intercettazioni come mezzo di prova a fini di giustizia sono ammesse. I riferimenti normativi sono il Codice di Procedura Penale e una legge sulla *criminal intelligence*. Il giudice delle indagini preliminari, su richiesta del procuratore, può ordinare il tracciamento di una persona, di un veicolo o di una cosa di altro genere e può ordinare anche la registrazione audio o video durante il periodo della sorveglianza. È altresì consentito carpire informazioni attraverso il computer dei soggetti sottoposti a intercettazioni. Il provvedimento del giudice delle indagini preliminari deve essere motivato e argomentato. Si ricorre a strumenti di questo tipo per le investigazioni su reati gravissimi, gravi, con aggravanti, nonché per taluni reati di minore importanza. Questi ultimi, tuttavia, non rientrano tra i casi per cui è consentito carpire informazioni attraverso il computer dell'indagato.

Le intercettazioni sono eseguite dal Dipartimento di Polizia o da altre strutture pubbliche (ad es. Guardia di Finanza, Polizia di frontiera, eccetera), secondo le disposizioni della legge sulla *criminal intelligence*. La durata della sorveglianza in segreto non può superare i sei mesi, tranne che quando si tratta di reti criminali su larga scala, nel qual caso si può arrivare a nove mesi.

Le informazioni raccolte sono utilizzate per la redazione di un rapporto e, immediatamente dopo, vengono distrutte quelle sulla vita privata e quelle comunque non attinenti al processo penale. Le decisioni riguardanti la distruzione sono prese dal procuratore alla scadenza dei termini per ricorsi e appelli contro le procedure seguite nell'indagine preliminare. In altri casi le registrazioni sono conservate dal procuratore e messe a disposizione del giudice, a richiesta da parte della corte giudicante.

Il principio della riservatezza va osservato in tutte le fasi del procedimento penale. Soltanto i funzionari responsabili hanno diritto di lavorare con le informazioni classificate.

Le informazioni ottenute tramite intercettazioni in occasione di un procedimento penale sono utilizzabili anche in altri procedimenti penali, previa decisione in tal senso da parte del procuratore generale. Se il procedimento penale originario è in svolgimento, l'eventuale utilizzazione delle intercettazioni anche in altri procedimenti è decisa dal giudice delle indagini preliminari oppure dalla corte del tribunale che sta celebrando il processo.

Sono consentite anche intercettazioni a scopo di prevenzione di un reato. In tal caso non occorre che l'indagine preliminare sia già iniziata, tuttavia essa può essere aperta immediatamente dopo l'acquisizione di indizi d preparazione di un reato.

Non si hanno notizie di fonte ufficiale in merito ai costi delle intercettazioni.

Lussemburgo

In Lussemburgo le intercettazioni possono essere usate come mezzo di prova in tribunale, a condizione che fossero state debitamente autorizzate. I principali riferimenti normativi in materia di intercettazioni sono il Codice di Procedura Penale e una legge dell'anno 2016 sull'*Intelligence Service.* È il magistrato che conduce le indagini preliminari ad autorizzare le intercettazioni eseguite dalla Polizia, mentre se si tratta di intercettazioni ad opera dell'*Intelligence Service* allora devono essere autorizzate da una speciale commissione, il *Departmental Intelligence Committee*.

Le intercettazioni possono durare un mese ma sono consentiti rinnovi dell'autorizzazione fino ad arrivare a un anno completo e, anzi, a tredici mesi se ciò viene ordinato in forma motivata dal giudice delle indagini preliminari, con l'assenso del presidente della camera di consiglio della corte d'appello, sentito il Procuratore di Stato.

Se le intercettazioni non hanno dato risultati utili, saranno distrutte, e così pure i relativi dati e informazioni. Alla distruzione provvede il giudice delle indagini preliminari, entro dodici mesi dalla cessione dell'intercettazione. Se invece sono risultate rilevanti, il giudice ordina di conservarle per il prosieguo delle investigazioni, tuttavia l'indagato o il Procuratore di Stato possono opporsi. Quando la sentenza del procedimento penale dell'imputato è diventata definitiva, quale che essa sia -di condanna o di assoluzione- registrazioni e dati saranno distrutti a cura del Procuratore Generale di Stato o del Procuratore di Stato, entro un mese.

È vietata la diffusione di filmati, registrazioni e ogni genere di elemento ottenuto per mezzo delle intercettazioni ma non rilevante ai fini del procedimento penale.

L'utilizzabilità delle intercettazioni vale esclusivamente per il procedimento penale in relazione al quale esse sono state autorizzate.

La raccolta di informazioni in segreto non è consentita. Qualora una persona stia svolgendo attività criminali, il procuratore generale (*attorney general*) può ordinare alla polizia un'investigazione e l'adozione di tutte le misure consentite dalla legge.

Non ci sono informazioni precise di fonte riguardo ad una serie di questioni: la conservazione delle informazioni acquisite per mezzo delle intercettazioni, la responsabilità e i criteri relativi alle valutazioni sulla rilevanza o no dei risultati delle intercettazioni, l'applicabilità o no delle norme sulle intercettazioni al prelevamento di dati dai computer degli indagati, l'ammissibilità o no di intercettazioni finalizzate alla prevenzione di un reato, i costi delle intercettazioni.

Macedonia

In Macedonia le intercettazioni sono considerate misure investigative speciali e possono essere utilizzate come mezzo di prova a fini giudiziari. Secondo il Codice di Procedura Penale, che è il basilare riferimento normativo in materia unitamente ad una legge del 2018 sull'intercettazione delle comunicazioni, si definiscono intercettazioni in senso stretto l'acquisizione e la registrazione di comunicazioni telefoniche o supportate da altri strumenti elettronici. Sono peraltro ammessi ulteriori tipi di intercettazione e acquisizione di informazioni tra cui: intercettazioni ambientali presso il domicilio degli indagati, registrazioni nelle vicinanze di esso, accesso segreto ai loro computer, accesso ai loro metadata telefonici o di natura elettronica di altra natura, infiltrazioni di agenti sotto falsa identità all'interno di organizzazioni criminali.

Le misure investigative speciali -e dunque le intercettazioni- possono essere disposte soltanto per determinate categorie di reati elencate dalla legge, che sono numerose. Tra queste: reati che comportano la detenzione per un periodo superiore a quattro anni commessi da bande e criminalità organizzata; omicidi, sequestri, sfruttamento della prostituzione, narcotraffico, reati contro il patrimonio culturale, riciclaggio di denaro, contrabbando, corruzione, terrorismo e altro ancora.

Le intercettazioni sono autorizzate dal giudice delle indagini preliminari, su richiesta da parte del procuratore, o da parte della polizia attraverso il procuratore. L'esecuzione delle intercettazioni è compito della polizia giudiziaria la quale, per gli aspetti tecnologici dell'operazione, si avvale di un'agenzia apposita, denominata *Operational and Technical Agency*. La durata iniziale delle intercettazioni è di quattro mesi, ma può essere estesa di altri quattro sulla base di una richiesta motivata, e può allungarsi ulteriormente di qualche mese per i reati commessi dalla criminalità, ma in nessun caso potrà superare la soglia di quattordici mesi complessivi.

I dati raccolti sono immagazzinati dal procuratore, che decide quali vanno trasmessi alla corte giudicante. Il procuratore può anche decidere la chiusura dell'indagine e, in tale evenienza, mette i dati delle intercettazioni a disposizione del giudice delle indagini preliminari. Per i dati da distruggere si prepara un rapporto. La distruzione è decretata dal giudice delle indagini preliminari, che di ciò fa apposita richiesta agli uffici, e viene seguita da un giudice nominato dal tribunale territorialmente competente. Il personale che per motivi di lavoro viene a conoscenza dei contenuti delle intercettazioni è tenuto al segreto. Chi viene a conoscenza di illegalità nell'acquisizione di intercettazioni deve denunciare il fatto. La diffusione di filmati o di registrazioni non rilevanti per il processo è punita con la reclusione da uno a cinque anni.

I contenuti ricavati dalle intercettazioni sono utilizzabili solo per il procedimento in corso. Se dalle intercettazioni emergono reati diversi da quelli ipotizzati in partenza, le evidenze impreviste sono utilizzabili a condizione che si tratti di reati inclusi nella casistica prestabilita dalla legge (vedi sopra). Le

intercettazioni preventive sono consentite, di nuovo con riferimento alla casistica indicata dalla legge nonché in poche altre ipotesi particolari.

Non si hanno informazioni di fonte ufficiale sui costi delle intercettazioni.

Norvegia

In Norvegia le intercettazioni a fini di giustizia sono lecite. La materia è regolata dal Codice di Procedura Penale e, per quanto attiene al trattamento delle informazioni raccolte, dal *Police Register Act*.

Le intercettazioni sono autorizzabili soltanto se si presume che il loro apporto all'indagine sia essenziale e che esse non siano surrogabili con altri mezzi.

Le intercettazioni consistono nell'ascolto di conversazioni o comunicazioni per mezzo di strumenti elettronici.

Il tribunale autorizza le intercettazioni nei confronti di chi è ragionevolmente sospettato di avere commesso un reato oppure di avere intenzione di commetterlo. In caso di estrema urgenza l'autorizzazione può essere data dal procuratore e iniziata immediatamente; in tal caso sarà necessario che entro ventiquattro ore il procuratore inoltri al tribunale il suo provvedimento, per l'approvazione da parte di quest'ultimo organo. L'esecuzione delle intercettazioni spetta alla polizia. La polizia può ordinare al gestore di un network o di un servizio di fornire la necessaria collaborazione tecnica. Né il soggetto interessato né altre parti in causa devono essere avvisate dell'intercettazione in corso.

L'autorizzazione ad intercettare viene concessa per il tempo strettamente indispensabile, è rinnovabile, e vale per non più di quattro settimane alla volta. La durata di un periodo di intercettazione può salire fino a otto settimane solamente se sono a rischio l'autonomia o gli interessi fondamentali del Paese (i quali sono indicati dal Capitolo 17 del Codice Penale).

Il trattamento delle informazioni ottenute mediante l'intercettazione è affidato alla polizia e alla procura, che svolgono tale compito conformemente alla legge. Polizia e procura sono responsabili della selezione dei dati e delle informazioni rilevanti all'interno del materiale raccolto. Il trattamento delle informazioni da parte della polizia e della procura è supervisionato da un comitato di controllo, formato da un minimo di tre membri, nominati dal Re della Norvegia. Tra i poteri del comitato vi è quello di convocare il personale della polizia e della procura per spiegazioni circa il loro operato. Al comitato di controllo non possono essere opposti segreti. Tuttavia, il controllo da parte del comitato non si applica al settore *dell'intelligence* e dei servizi di sicurezza.

Tutti coloro che, a vario titolo, hanno partecipato a un'operazione di intercettazione o alle relative procedure autorizzative sono tenuti al segreto al di fuori dell'ambito investigativo e giudiziario per il quale l'intercettazione è stata realizzata. Questo vale anche per le informazioni di cui sono venuti a conoscenza. Essi dovranno mantenere il segreto verso l'esterno anche per quanto concerne informazioni e dati sulla vita privata delle persone intercettate.

A fini di indagine e di giustizia, è consentito l'accesso in segreto nei computer delle persone sospettate, sempre per il tempo minimo indispensabile.

Le intercettazioni possono essere usate come mezzo di prova di reati diversi da quello per il quale erano state predisposte, a condizione che anche per questi ultimi

ricorrano le condizioni generali stabilite dalla legge. Le intercettazioni finalizzate alla prevenzione dei reati sono consentite.

Non sono disponibili informazioni sui costi delle intercettazioni.

Polonia

In Polonia le intercettazioni e le registrazioni di conversazioni telefoniche possono avvenire o in relazione ad un procedimento giudiziario pendente, e in tal caso si parla di modalità procedurale, o nel contesto di un'operazione di controllo, vale a dire in modalità operativa. Nella modalità operativa, possono essere oggetto di intercettazioni e registrazioni anche immagini e suoni provenienti da edifici, da mezzi di trasporto, da luoghi non pubblici, nonché la corrispondenza cartacea ed elettronica, i dati contenuti nei computer o immagazzinati nei sistemi di comunicazione, i contenuti delle spedizioni.

Le intercettazioni e registrazioni secondo modalità procedurale sono ordinate dal tribunale, ai sensi del codice di procedura penale, su richiesta del procuratore; le intercettazioni e registrazioni in modalità operativa sono anch'esse ordinate dal tribunale, ma ai sensi di leggi speciali e su richiesta, in questi casi, presentata dagli apparati autorizzati a condurre operazioni di controllo e investigative, previo assenso da parte del procuratore. Gli apparati in questione sono: Polizia, Agenzia per la Sicurezza Interna, Ufficio per la Sorveglianza Interna, Ufficio Centrale Anticorruzione, Amministrazione Nazionale delle Entrate, Servizio di *Counterintelligence* Militare, Servizio di Protezione dello Stato, Polizia di Frontiera, Polizia Militare, Ispettorato Interno dei Servizi Penitenziari.

Nella modalità procedurale, che fa riferimento al Codice di Procedura Penale, intercettazioni e registrazioni di contatti telefonici sono legittime a condizione che i processi pendenti o fondati timori di nuovi delitti in preparazione riguardino una tipologia di reati inclusa tra quelle -assai numerose- elencate dall'articolo 237 del Codice stesso. Nella modalità operativa, sono legittime a condizione che ciascuno degli apparati autorizzati a condurre operazioni di controllo e investigative si attenga alla tipologia di reati che gli compete.

All'esecuzione delle intercettazioni provvedono le società di telecomunicazioni, che per legge (*Telecommunications Act*) sono obbligate a collaborare.

La durata delle intercettazioni, se in modalità procedurale, è di tre mesi, con possibilità di proroga per altri tre mesi in presenza di giustificato specifico motivo; se in modalità operativa altrettanto, ma con la differenza che in casi particolari l'estensione può arrivare ad un totale di dodici mesi per la Polizia e la maggior parte degli apparati legittimati, e anche oltre per Agenzia per la Sicurezza Interna e per il Servizio di *Counterintelligence* Militare.

Quanto alla conservazione e all'utilizzazione di dati e informazioni raccolti, nella modalità procedurale il procuratore seleziona il materiale interessante per il processo, che mette a disposizione del tribunale, e redige una domanda di distruzione di tutto il resto, che sarà esaminata dal tribunale. Nella modalità operativa, in linea di massima ciascuno degli apparati distrugge i materiali non interessanti: tra le eccezioni, la più rilevante sembra quella relativa ad operazioni condotte ai fini della sicurezza dello Stato, per le quali la Corte distrettuale di

Varsavia può decidere, con provvedimento scritto, di conservare comunque gli elementi raccolti.

La divulgazione è punita, con sanzioni pecuniarie o carcerarie. È punita anche la divulgazione indiretta, ovvero il caso in cui il pubblico ufficiale non divulghi direttamente bensì fornisca ad estranei il materiale che poi questi ultimi divulgano.

Circa l'utilizzabilità in altri procedimenti delle informazioni attinte, decide il procuratore.

Non si hanno informazioni attendibili sui costi e su chi se ne faccia carico.

Portogallo

In Portogallo le intercettazioni possono essere un mezzo di prova a fini giudiziari. Si possono intercettare telefonate, comunicazioni trasmesse per mezzo di strumenti diversi dal telefono, -tra cui le e-mail e le trasmissioni telematiche di dati- e comunicazioni che avvengono di persona. È quindi legittimo operare anche sui computer.

Il riferimento normativo basilare in materia è il Codice di Procedura Penale.

In un'inchiesta, le intercettazioni possono essere autorizzate soltanto a condizione che vi siano elementi per ritenerle indispensabili ai fini dell'accertamento della verità e non surrogabili per mezzo di altri metodi di indagine. Inoltre il reato in relazione al quale si intende disporre un'intercettazione deve rientrare tra quelli elencati, per categorie, dall'articolo 187 del Codice di Procedura Penale: reati puniti con la carcerazione per più di tre anni, reati connessi alla droga, possesso illecito e traffico di armi, contrabbando, ingiurie, minacce (anche con la commissione di un reato o abuso), coercizione, violazioni della riservatezza, molestie e disturbi vari per mezzo del telefono, procurato allarme, intralcio alla giustizia (da parte di un condannato per i reati di cui sopra).

L'autorizzazione viene formalizzata con un provvedimento emanato dal giudice competente su richiesta della procura. Le intercettazioni, così autorizzate, possono essere eseguite soltanto dalla polizia. L'intercettazione ha una durata di tre mesi ed è rinnovabile per altri tre.

I materiali ottenuti attraverso le intercettazioni sono conservati dalla polizia, e più precisamente dagli uffici di polizia che l'hanno eseguita. Per la selezione degli elementi rilevanti e la loro distinzione da quelli che non lo sono, la polizia stende un rapporto che trasmette alla procura, la quale ne prende visione e inoltra tali elementi di valutazione nonché i materiali al giudice, che prende la decisione finale. Se necessario, in questa fase il giudice si farà assistere da personale della polizia ed eventualmente anche da un interprete. Il giudice ordina la distruzione immediata di ciò che palesemente non è di interesse per il processo.

I contenuti delle intercettazioni non possono essere usati in procedimenti diversi da quello per cui sono state fatte.

Non sono consentite intercettazioni preventive. Le intercettazioni devono sempre essere relative ad un'inchiesta già aperta.

Non si hanno notizie ufficiali sui costi delle intercettazioni.

Regno Unito

Nel Regno Unito le intercettazioni, a seconda della tipologia, possono consistere sia in un mezzo di ricerca della prova che in un vero e proprio mezzo di prova e possono pertanto rispondere a finalità di supporto dell'attività giudiziaria o di prevenzione del crimine. La fonte recante la disciplina principale delle intercettazioni, nota come "IPA"[70], distingue diverse metodologie di acquisizione delle comunicazioni: intercettazione di comunicazioni[71]; accesso ai dati di comunicazioni[72]; interferenza con apparecchiature[73] e interferenza nella proprietà[74]. Viene espressamente escluso[75] che le "intercettazione di comunicazioni" possono costituire dei mezzi di prova in un procedimento giudiziario[76], mentre il materiale ottenuto attraverso l'interferenza di apparecchiature, di proprietà o dai dati di comunicazione può essere utilizzato come oggetto di prova in sede processuale. La durata del mandato per le operazioni di intercettazione delle comunicazioni, in particolare, è prevista dall'articolo 32 dell'IPA. Per quanto concerne la disciplina delle procedure di "stoccaggio" del materiale acquisito, essa si rinviene nel "equipment interference Code of Practice", mentre gli articoli 53[77] e 54 dell'IPA contengono garanzie relative alla conservazione e alla divulgazione del materiale intercettato. L'articolo 57 dell'IPA,

[70] Investigatory Powers Act 2016 disciplina i poteri della polizia e di altri enti pubblici competenti ad acquisire "dati sulle comunicazioni" e il contenuto degli stessi. La disciplina della "'interferenza sulla proprietà" viene invece riservata alla parte III del Police Act 1997.

[71] Nella parte II, S15, l'IPA riserva a talune autorità la facoltà di ottenere il mandato per eseguire intercettazioni di comunicazioni, comprese quelle trasmesse da un sistema di telecomunicazione, di accedere al loro contenuto e di ottenere i relativi dati secondari. S20 dell'IPA prevede che i mandati siano approvati per motivi di sicurezza nazionale, prevenzione o individuazione di reati gravi e nell'interesse del benessere economico del paese. I mandati per queste operazioni sono concessi dalla Segreteria di Stato e approvati da un Commissario Giudiziario. Possono richiedere l'emissione di un mandato e, quindi, condurre un'operazione di intercettazione delle comunicazioni i soli soggetti specificamente individuati dall'Investigatory Powers Act 2016, S18.

[72] Dalla parte III, S61, dell'IPA, l'accesso viene consentito alle autorità pubbliche, ove necessario, per vari scopi specifici, tra cui anche la prevenzione e l'accertamento di reati. I dati di comunicazione, secondo il codice di condotta, includono il "chi", il "quando", il "dove" e il "come" di una comunicazione ma non il suo contenuto. l'Ufficio per le autorizzazioni sui dati delle comunicazioni (OCDA) è l'organismo deputato alle relative richieste e svolge tale ruolo per conto del Commissario per i Poteri Investigativi.

[73] La parte 5 dell'IPA consente ai capi di polizia, come elencati nel S6 dell'IPA, di rilasciare mandato ai loro ufficiali per esercitare una "interferenza con apparecchiature mirate" (ad es. hackerare) di altre apparecchiature al fine di ottenerne comunicazioni o dati. A norma del S106(1) dell'IPA, gli ufficiali superiori devono valutare se il mandato sia necessario al fine di prevenire o individuare reati gravi, o in situazioni di pericolo per la vita, se l'attività risulti proporzionata e se sussistano garanzie che assicurino che i dati, una volta ottenuti, siano trattati in modo appropriato.

[74] I capi della polizia, come previsto dal S95(5) del Police Act 1997, possono conferire mandato per "interferire", ovvero accedere, nella proprietà o nella "telegrafia senza fili" (ad esempio i telefoni) di coloro che sono sospettati di aver commesso gravi reati.

[75] S56 of the Investigatory Powers Act 2016

[76] Secondo un portavoce del Ministero dell'Interno, il materiale intercettato può essere reso noto al giudice solo "*in circostanze del tutto eccezionali... ad esempio se potesse scagionare l'imputato*".

[77] In particolare, si prevede che i materiali ottenuti debbano essere *"distrutti non appena non sussistono più motivi rilevanti per trattenerli*", specificandone le circostanze, S53(6 to 7) dell'IPA.

inoltre, prevede l'obbligo di non effettuare divulgazioni non autorizzate del materiale intercettato e che il mancato rispetto di tale obbligo costituisca un reato punibile con la reclusione fino a 12 mesi e/o con una multa illimitata.

Romania

Le intercettazioni, mezzi di prova in sede processuale, devono essere effettuate nel rispetto della disciplina di diritto penale e dalle altre leggi connesse[78]. Le intercettazioni telefoniche o di altre tipologie di conversazioni consistono in strumenti di sorveglianza tecnica (in funzione cautelare rispetto alla futura commissione di reati) e, allo stesso tempo, in metodi speciali di ricerca (di materiale probatorio) e di vigilanza (che concorrano all'identificazione o alla localizzazione delle persone). Il Centro nazionale per l'intercettazione delle comunicazioni, del servizio di intelligence romeno[79], su richiesta delle autorità investigative, assicura ai fornitori di servizi di comunicazioni elettroniche destinate al pubblico l'accesso diretto e autonomo ai sistemi tecnici per l'espletamento della vigilanza prevista dall'art. 138, par.1), lett. a), dal codice di procedura penale[80]. Sul regime delle spese processuali, provvede l'art. 272 del codice di procedura penale.

[78] L'art. 139 della legge n. 135/2010, codice di procedura penale, nello specifico, prevede che la sorveglianza tecnica possa essere disposta, al ricorrere di determinati presupposti, per una serie di reati puntualmente elencati e, comunque, in caso di reati per i quali la legge preveda la pena della reclusione non inferiore a 5 anni. Le registrazioni costituiscano mezzi di prova nel processo a carico dell'imputato quando riguardino conversazioni o comunicazioni avute con terzi. Qualsiasi altra registrazione può costituire una prova a meno che non sia vietata dalla legge. L'art. 140 del codice, nel dettare la disciplina dell'iter autorizzativo, prevede che la sorveglianza tecnica possa essere disposta su richiesta del pubblico ministero nel corso dell'istruttoria, per una durata massima di 30 giorni, o dal giudice dei diritti e delle libertà del tribunale competente o dal tribunale nel cui circondario ha sede la procura di cui fa parte il pubblico ministero. L'art. 141 consente al pubblico ministero di autorizzare misure tecniche di sorveglianza per una durata massima di 48 ore ove ne sussista l'urgenza. A norma dell'art. 142, la sorveglianza tecnica è eseguita dal pubblico ministero, sebbene questi possa delegare all'organo investigativo o a personale specializzato della polizia (assicurando l'utilizzo di procedure idonee a garantire l'integrità e la riservatezza delle informazioni raccolte). I fornitori di reti pubbliche di comunicazione elettronica sono tenuti a collaborare e hanno l'obbligo di mantenere il segreto sull'operazione compiuta, incorrendo altrimenti in sanzioni di natura penale. I dati acquisiti dalle operazioni di sorveglianza tecnica possono essere utilizzati anche in altri procedimenti penali se apportino dati utili o informazioni circa la preparazione o commissione di altri reati tra quelli previsti dall'art. 139, mentre i dati raccolti che non riguardino il fatto oggetto di indagine o che non contribuiscano all'identificazione o alla localizzazione delle persone, se non utilizzati in altri procedimenti, vengono archiviati presso la Procura. Trascorso un anno dalla definizione del giudizio, i dati devono essere distrutti dal pubblico ministero. La misura della sorveglianza tecnica può essere prorogata, sulla base di fondati motivi, dal giudice dei diritti e delle libertà dal tribunale competente, su richiesta motivata del pubblico ministero, se ricorrono i presupposti previsti dall'art. 139. Ciascuna proroga non può essere superiore a 30 giorni. La durata complessiva delle operazioni di sorveglianza tecnica non può superare 6 mesi, ad eccezione della misura di audio/video/foto sorveglianza in ambienti privati, che non può eccedere i 120 giorni (art. 144). A norma dell'art. 145 del codice, cessata la misura della sorveglianza, entro 10 giorni, il pubblico ministero informa ciascun soggetto interessato del mandato emesso nei suoi confronti.

[79] Il servizio di intelligence, a tutela della sicurezza nazionale, è autorizzato a detenere e utilizzare mezzi idonei a carpire, verificare, elaborare e archiviare informazioni.

[80] Gli artt. 9-11 della legge n. 14/1992 contengono la specifica disciplina.

Slovacchia

In Slovacchia le intercettazioni sono concepite come un mezzo di ricerca della prova, disciplinate dalla legge sulla protezione contro le intercettazioni e dal codice di procedura penale[81]. Le intercettazioni possono essere utilizzate in sede penale solo per i reati la cui cornice edittale della pena detentiva sia superiore, nel massino, a 5 anni e per talune specifiche fattispecie delittuose[82]. Un mandato di intercettazione e registrazione di telecomunicazioni può essere emesso ove sia possibile presumere che contribuiscano a far acquisire tutti i fatti rilevanti per il procedimento penale[83]. Le intercettazioni devono essere autorizzate da un tribunale e sono eseguite dalle forze di polizia, dal servizio di informazione slovacco, dall'intelligence militare, dal servizio di guardia carceraria e giudiziaria e dall'ufficio delle dogane[84]. La durata massima dell'autorizzazione è di sei mesi, ma può essere prorogata dal tribunale fino ad altri sei, a fronte di una richiesta scritta. Non è previsto un limite al numero di proroghe concedibili. Durante il procedimento penale, nella specie durante la fase istruttoria, la durata delle intercettazioni è fissata a sei mesi. Tuttavia, su richiesta del pubblico ministero, può essere concessa una proroga di due mesi (ripetutamente) dal giudice delle indagini preliminari. Le registrazioni di telecomunicazioni, nella loro integrità, devono essere conservate in un archivio, che assicura idonei supporti elettronici, da cui potrà essere estratta copia ad opera del pubblico ministero, dell'imputato o del suo difensore. La riservatezza delle attività di intercettazione viene garantita poiché l'accesso viene concesso ad un numero limitato di persone e sono previste conseguenze disciplinari e penali in caso di inosservanza e "fughe". Può essere avviato un procedimento disciplinare o penale per la diffusione di filmati, registrazioni o materiale ottenuto tramite intercettazioni e non attinente ai procedimenti giudiziari. Alla distruzione delle registrazioni provvede, nei modi prescritti e senza indebito ritardo, l'autorità giudiziaria o il competente dipartimento delle forze di polizia[85]. Le intercettazioni possono essere utilizzate come strumento di prevenzione della commissione di reati[86].

---

81 Art. 119, lett. 3, della legge n. 301/2005, codice di procedura penale, ove sono definite "mezzi tecnico-informatici", e dalla legge n. 166/2003, Racc. sulla protezione della vita privata contro l'uso non autorizzato di mezzi informatici.

82 Quali corruzione; reati di estremismo; di abuso d'ufficio di pubblico ufficiale; di riciclaggio ai sensi degli artt. 233 e 234 del codice penale o altro reato doloso, la cui esecuzione sia imposta da un trattato internazionale.

83 Lo prevede l'art. 115, n. 1, del codice di procedura penale. Le intercettazioni, ai sensi dell'art. 115 n. 7, possono essere utilizzate anche in altri procedimenti qualora il reato rientri nell'ambito di applicazione di cui all'articolo 115 n. 1 del codice.

84 Articolo 2, n. 2, della legge sulla protezione contro le intercettazioni.

85 Articolo 115, comma 8, del codice di procedura penale.

86 È previsto dall'art. 3, n. 1, della legge sulla protezione contro le intercettazioni.

Slovenia

Le intercettazioni telefoniche sono una delle misure investigative segrete che, nel rispetto delle disposizioni della legge di procedura penale, possono interferire con la garanzia costituzionale di cui all'art. 38 della Costituzione della Repubblica di Slovenia ove sussistano ragionevoli motivi per sospettare che qualcuno abbia commesso, stia commettendo o stia preparando e/o organizzando la commissione di determinati reati[87]. Le intercettazioni devono essere disposte con ordinanza motivata del giudice per le indagini preliminari su istanza del pubblico ministero. L'ordine del giudice istruttore è poi eseguito dalla polizia, con cui gli operatori delle comunicazioni elettroniche sono obbligati a collaborare. Il termine per il compimento dell'operazione decorre dal momento in cui viene disposto il primo provvedimento e può durare al massimo sei mesi, al termine del quale, l'operazione può essere avviata nei confronti dello stesso indagato solo al fine di accertare un altro reato. Il materiale raccolto è "stoccato" in conformità a quanto prescritto dagli artt. 153 e 154 della legge di procedura penale[88]. Le forze dell'ordine, al fine di evitare un'eventuale "fuga di notizie" che rischierebbe di pregiudicare le indagini in corso o future, adottano una procedura speciale per assicurare il buon esito delle operazioni di intercettazione[89]. L'intercettazione di comunicazioni elettroniche, così come la loro registrazione[90], può riguardare tutte le forme di comunicazione trasmesse dai moderni dispositivi elettronici. Nell'attuare queste misure, la polizia segue regole interne specifiche. L'utilizzazione delle intercettazioni è limitata al procedimento in cui sono disposte dal giudice istruttore e non possono essere impiegate come strumento di prevenzione del crimine. I costi delle intercettazioni sono gestiti dalla polizia alla luce della disciplina sull'attuazione di misure investigative segrete.

---

87 Sono consentite solo nei casi e per i reati previsti dall'art. 150 della legge di procedura penale (http://www.pisrs.si/Pis.web/cm?idStrani=prevodi). In particolare, nell'ambito della criminalità organizzata, ove i reati non possano essere individuati in altro modo, è possibile far ricorso in via eccezionale alle misure investigative coperte (es. falsa identità e titolarità di beni, sorveglianza occulta, ottenimento dei dati relativi al traffico delle comunicazioni elettroniche, controllo della corrispondenza, intercettazioni, ecc.).

88 Al termine delle operazioni (anche se le indagini sono ancora in corso), la polizia è tenuta a consegnare al pubblico ministero tutto il materiale raccolto attraverso l'uso di tali misure, unitamente ad un verbale riassuntivo delle prove raccolte (trascrizioni delle relative comunicazioni). Nessuna registrazione può essere conservata dalla polizia. Il materiale viene mantenuto dal giudice per tutto il tempo in cui viene conservato il fascicolo del relativo procedimento penale. Nell'evenienza in cui il pubblico ministero decida di archiviare ovvero se, entro due anni dall'ultimo dei provvedimenti richiamati, non presenti alcun atto di accusa o diretto a perseguire l'indagato, il materiale deve essere distrutto sotto la vigilanza del giudice istruttore. Prima della distruzione, il giudice istruttore dà comunicazione ai soggetti interessati.

89 È prevista una pena per chi diffonda filmati, registrazioni o materiale ottenuto mediante intercettazioni e non attinente al procedimento.

90 Di cui all'art.150, comma 1, n. 1, della legge di procedura penale.

Svezia

Le intercettazioni, quali mezzi di ricerca della prova[91], possono essere disposte durante le indagini preliminari in presenza di determinate fattispecie delittuose[92] ed avere ad oggetto dati e comunicazioni elettroniche (in presenza di reati per i quali è prevista una pena detentiva non inferiore nel minimo a due anni) o avvenire in luoghi privati (in ipotesi di reati per i quali è prevista una pena minima di quattro anni di reclusione). Le intercettazioni vengono disposte dall'autorità giudiziaria a fronte della richiesta del pubblico ministero e sono eseguite dalle forze di polizia. La durata non può eccedere un mese dalla data in cui fu conferito mandato[93]. Le registrazioni devono essere conservate fino al termine delle indagini o del giudizio, potendo essere trattenute anche a fini cautelari, per poi essere distrutte dal pubblico ministero[94]. Per quanto riguarda la riservatezza[95], è previsto che un funzionario che nell'esercizio delle sue funzioni trasgredisca ai suoi doveri possa incorrere nella pena di una multa o della reclusione fino a due anni, mentre un funzionario che riveli informazioni segretate o chi sfrutti illecitamente tale segreto si rende colpevole di violazione del dovere di riservatezza ed è condannato ad una multa o alla reclusione per un massimo di un anno[96]. Le prove ottenute mediante le intercettazioni sono inserite nell'istruttoria ad opera del pubblico ministero, che ne dà comunicazione all'imputato e ai difensori, e, al ricorrere di determinate circostanze, può decidere di utilizzare informazioni raccolte anche se non correlate al reato per cui l'autorizzazione fu concessa[97]. Le intercettazioni possono essere utilizzate anche come strumento di prevenzione del crimine[98]. Le spese per le intercettazioni sono a carico dell'autorità investigativa.

---

91 La disciplina, concernente i reati per i quali le intercettazioni possono essere richieste e la relativa procedura operativa, è contenuta nel codice svedese di procedura giudiziale e nella legge sul recupero dati (n. 62/2020). Le intercettazioni telefoniche, in particolare, possono avvenire come intercettazioni segrete di comunicazioni elettroniche, di cui all'art. 18, cap. 27, del codice di procedura; di discorsi e conversazioni private, come intercettazioni segrete "della stanza/spazio", di cui all'art. 20, cap. 27, del codice o come intercettazioni occulte dei dati, di cui all'art. 1 della legge sul recupero dati.

92 Ad es. alto tradimento, spionaggio, reati terroristici e reati violenti gravi.

93 Articolo 21, cap. 27, del codice di procedura giudiziale e articolo 18 della legge sul recupero dati.

94 Articolo 24 del codice di procedura giudiziale e articolo 28 della legge sul recupero dati. Il materiale ricavato dalle intercettazioni, secondo il "Criminal Data Act" (legge n. 1177/2018) e il "Processing Act" (legge n. 1693/2018), può essere trattenuto ed elaborato dall'autorità di polizia se necessario per prevenire, scoraggiare o individuare attività criminali.

95 Vi sono disposizioni di particolare rilevo al capitolo 18 della legge sull'accesso pubblico alle informazioni e segretezza "Public access to information and secrecy – The legislation in brief (SwedishMinistryofJustice,2020)",p.3e24,https://www.regeringen.se/4aaa1c/contentassets/f381325faa3b41dc859080a0b1b4c994/public-access-to-information-and-secrecy.pdf.

96 Articolo 1 e 3, cap. 20, del codice penale svedese.

97 La disciplina operativa è contenuta nell'articolo 4, cap. 23, del codice svedese di procedura giudiziale; nella guida legale all'ufficio del pubblico ministero (n. 26/2022), p. 13 e p. 36-37; nel Cap.10, artt. 3–4, della legge sull'accesso pubblico all'informazione e segretezza (legge n. 400/2009).

98 La legislazione preventiva è costituita principalmente dalla legge sulla prevenzione (legge n. 979/2007) e dalla legge sulle intercettazioni (legge n. 278/2012), normativa in costante aggiornamento, per l'introduzione di nuove misure coercitive occulte (legge sul trattamento dei dati) "Intermediary report (SOU 2022:52) – *The report on extended possibilities to use preventive cov-ert coercive measures"*

(disponibile solo in Svedese*)*. La legge sull'intercettazione consente alle forze dell'ordine, in determinate circostanze, di recuperare informazioni da fornitori di servizi di rete per le comunicazioni elettroniche ai sensi della legge sulle comunicazioni elettroniche (legge n. 389/2003). Tali decisioni vengono prese dai pubblici ministeri su richiesta delle forze dell'ordine (artt.1–3della legge sulle intercettazioni).

Svizzera

Le intercettazioni sono un mezzo di ricerca e conservazione della prova[99] e possono essere utilizzate esclusivamente nell'ambito dei procedimenti penali aventi ad oggetto i reati elencati nell'art. 269, par. 2, del codice di procedura penale. A giustificare la misura devono concorrere non solo il forte sospetto che uno di tali reati gravi sia stato commesso, ma anche che le indagini, in loro assenza, non potrebbero avere alcuna prospettiva di successo o diverrebbero irragionevolmente complicate. Per tali ragioni, il loro utilizzo non può essere generalmente impiegato con funzione preventiva. Previa autorizzazione del tribunale dei provvedimenti coercitivi[100], possono essere disposte dalla procura, con durata non superiore a 3 mesi, pur potendo essere prorogate, anche più volte, nel rispetto del predetto limite[101]. È previsto che chiunque riveli o diffonda notizie segrete[102] sia punito con una pena detentiva non superiore a tre anni o con una pena pecuniaria[103]. In linea di principio, le intercettazioni telefoniche sono limitate ai procedimenti in cui sono disposte[104]. I documenti e i dati ottenuti dall'attività di intercettazione non autorizzata devono essere immediatamente distrutti e non possono essere utilizzati (art. 277 CrimPC).

[99] La disciplina è contenuta nel codice di procedura penale svizzero, nella legge federale sulla sorveglianza della corrispondenza e delle telecomunicazioni (nota con l'acronimo "SPTA", LINK) e nel relativo decreto (noto come "SPTO", LINK. In particolare l'art. 8 SPTO, rubricato "Registrazione delle telefonate come prova" reca la disciplina sulla procedura operativa). L'ufficio del pubblico ministero può disporle solo al ricorrere delle condizioni prescritte degli artt. 269 ss. del codice di procedura penale svizzero (CrimPC): LINK (in Francese) e conformemente alle condizioni generali di cui all'art. 197 CrimPC. Gli artt. 269*ter* e 269*quater* CrimPC (in Francese) disciplinano le condizioni per consentire di utilizzare il computer come captatore. Inoltre, l'art. 179*bis* del codice penale svizzero (LINK) proibisce la registrazione di conversazioni telefoniche senza il consenso dei soggetti interessati.

[100] Il Servizio di sorveglianza della posta e delle telecomunicazioni (PTSS), annesso al Dipartimento federale di giustizia e polizia, ha il compito di effettuare tale monitoraggio contattando gli operatori interessati al fine di raccogliere i dati che saranno poi trasmessi alle autorità giudiziarie penali.

[101] Se è richiesta una proroga, il pubblico ministero deposita la relativa istanza, motivandone le ragioni, prima della scadenza dell'autorizzazione in corso (art. 274, par. 5, CrimCP). Vige in ogni caso l'obbligo per il pubblico ministero di interrompe immediatamente le operazioni di intercettazione ove i presupposti vengono meno o l'autorizzazione, o la sua proroga, venga rigettata (art. 275 CrimCP).

[102] Di cui è venuto a conoscenza in qualità di pubblico ufficiale, membro di un'autorità, loro ausiliario o comunque nell'espletamento dei propri doveri d'ufficio.

[103] Al reato di violazione del segreto d'ufficio consegue la cessazione del rapporto di lavoro come membro di un'autorità o come pubblico ufficiale o come ausiliario (art. 320 codice penale svizzero).

[104] Art. 278 CrimPC (in Francese) disciplina il tema dei "ritrovamenti accidentali" (reati diversi da quelli previsti dall'ordinanza di sorveglianza) e specifica in quali circostanze tali informazioni possono essere utilizzate (in modo molto restrittivo e solo per rintracciare persone ricercate).

Turchia

In Turchia la ‘supervisione delle comunicazioni tramite tlc’ è una delle ‘misure di protezione’ applicabili per l’accertamento della verità nei procedimenti penali[105]. Se nell'ambito dell’indagine penale vi sono fondati motivi per ritenere che sia stato commesso un reato e non è possibile ottenere prove in altro modo, su decisione del giudice o, in caso di urgenza, del PM, è possibile intercettare e registrare le comunicazioni dell'indagato/imputato, nonché valutare le informazioni del segnale. Il reato è accertabile tramite qualunque prova legalmente ottenuta, pertanto le registrazioni audio/video raccolte ai sensi di legge possono essere utilizzate come mezzo di prova. Le misure comprendono: il rilevamento, l'intercettazione e la registrazione delle comunicazioni, la valutazione delle informazioni sul segnale e la localizzazione del telefono cellulare[106]. La misura è autorizzata dal giudice istruttore o, in caso di urgenza, dal PM, che sottopone immediata richiesta di convalida al giudice, chiamato a pronunciarsi entro 24 ore. L’autorizzazione viene emessa per massimo due mesi, prorogabili per un ulteriore mese; se necessario, il giudice può prorogare tali termini per non più di un mese alla volta e per un periodo complessivo non superiore a tre mesi. La misura, da mantenere riservata per l’intera operazione (la violazione comporta responsabilità penale) può applicarsi solo alle indagini sui reati più gravi: ad es. reati contro l’unità e l’integrità dello Stato, l’ordine costituzionale e il segreto di Stato, spionaggio, traffico di migranti, tratta, commercio di organi e tessuti, costituzione di organizzazioni a fini criminosi, omicidio, tortura, violenza sessuale. Spetta al giudice la selezione del materiale rilevante. Al fine di prevenire la commissione di reati, la Legge del 1934 sui doveri e i poteri della polizia consente (su decisione di un giudice o, in caso di urgenza, del Capo dell’intelligence o del Direttore generale della sicurezza o, limitatamente ai crimini informatici, del Capo dipartimento crimini informatici) la rilevazione e l’ascolto delle comunicazioni tramite tlc o il traffico di dati tra indirizzi di connessione a Internet e le fonti di Internet e i dati trasmessi, nonché la valutazione e registrazione delle informazioni del segnale. L'ordine scritto deve essere sottoposto ad approvazione del giudice e autorizzato entro 24 ore; il giudice deve decidere entro massimo 48 ore. Se il termine scade o il giudice decide diversamente, la misura viene revocata e le registrazioni distrutte entro 10 giorni; si redige verbale per eventuali ispezioni. La perquisizione, copia e sequestro di pc, programmi informatici e registri è consentita come misura di tutela penale distinta dalla sorveglianza delle comunicazioni. In merito all’utilizzabilità delle prove, il cpp non stabilisce che esse non possano essere utilizzate per altri

[105] Sono disciplinate dal Codice di procedura penale e dal Regolamento sulle procedure e i principi relativi all'individuazione, all'intercettazione, alla valutazione e alla registrazione delle comunicazioni tramite tlc.

[106] È possibile localizzare non solo il telefono cellulare utilizzato dall'indagato o dall'imputato, ma anche i cellulari non in suo uso, ma che potrebbero essere utili all’arresto. L'ordine di localizzazione di un cellulare può essere emesso per qualsiasi tipo di reato, senza limitazione ai reati elencati dal c.p.p. relativamente alla supervisione delle comunicazioni tramite tlc.

indagati o imputati nella medesima indagine; il cpp prevede, invece, che eventuali prove emerse tramite intercettazione in relazione alla commissione di reato non collegato alle indagini o all'azione penale in corso, devono essere conservate e la Procura immediatamente informata.

Ungheria

In Ungheria è previsto l'uso delle intercettazioni come mezzo di prova. Il principale riferimento normativo è il Codice di procedura Penale, ma ve ne sono anche altri (leggi e decreti). Sono consentite sia le intercettazioni e registrazioni di comunicazioni effettuate mediante reti e/o apparecchi elettronici, sia quelle informatiche. La raccolta di informazioni segrete a fini giudiziari può essere avviata prima ancora che un'indagine sia stata formalmente aperta, ai sensi del *Police Act* e del *National Tax and Customs Administration Act*.

Condizioni necessarie per effettuare un'intercettazione sono la ragionevole presunzione della sua indispensabilità, l'impossibilità di ottenere con altri mezzi le informazioni occorrenti, la garanzia che i diritti fondamentali di chi è sottoposto a intercettazione non siano compressi in misura sproporzionata rispetto agli scopi di giustizia perseguiti. Le intercettazioni devono essere autorizzate dalla magistratura.

Il codice di procedura penale indica le tipologie di reato per le quali le intercettazioni sono consentite. Si tratta di tutti i reati sanzionati con pene detentive dai cinque anni in su, nonché di numerosi reati per i quali la carcerazione sia almeno di tre anni.

I corpi dello Stato che possono procedere alle intercettazioni, sempre previa autorizzazione del giudice, sono molteplici: polizia, amministrazione doganale, procure, uffici anti-terrorismo, servizi di informazione e di sicurezza militare e altri ancora.

La durata delle intercettazioni è inizialmente di novanta giorni, ma possono esserci proroghe; al massimo si può arrivare a un anno. Anche le proroghe devono essere autorizzate dalla magistratura. Entro un mese dopo la fine dell'intercettazione, vengono cancellati i dati non riferibili allo scopo dell'intercettazione stessa e quelli non funzionali ai fini del procedimento penale. Per la conservazione, è stato creato un *Central Media Repository*. È vietato l'accesso alle intercettazioni (e alle relative registrazioni) di personale non autorizzato. È punito con la carcerazione chi ottiene illegalmente o usa informazioni classificate, chi le rivela, chi le nasconde all'autorità competente.

Per quanto concerne il da farsi con le informazioni ricavate per mezzo dell'intercettazione, il procuratore presenta le sue proposte al giudice, che decide con un provvedimento formale. È il giudice a stabilire se le intercettazioni siano avvenute legalmente e se siano utilizzabili nel processo. È consentito carpire informazioni entrando segretamente nel computer dell'indagato. Con riferimento alla persona nei confronti della quale è stata disposta l'intercettazione, i risultati dell'intercettazione stessa possono servire all'incriminazione anche per un altro reato, purché sia uno di quei reati contro i quali le intercettazioni sono ammesse. Per i reati inaspettati commessi invece da altra persona e rivelati dalle intercettazioni, si possono usare queste ultime nel caso di omicidi volontari, sequestri di persona, reati contro lo Stato, terrorismo, danni intenzionali alla

pubblica incolumità, a condizione che il procedimento penale supplementare sia iniziato entro otto giorni e che ci sia assenso da parte dell'autorità giudiziaria competente per il procedimento in funzione del quale era stata autorizzata l'intercettazione.

Le intercettazioni al fine di prevenire reati sono ammesse.

Non sono disponibili informazioni sui costi delle intercettazioni.