

# Sorveglianza da parte dei servizi di intelligence: garanzie dei diritti fondamentali e mezzi di ricorso nell'Unione europea

## Sintesi

*L'articolo 7 della carta dei diritti fondamentali dell'Unione europea garantisce ad ogni persona nell'Unione europea (UE) il diritto al rispetto della vita privata e familiare, mentre l'articolo 8 garantisce il diritto alla protezione dei dati di carattere personale che la riguardano. Detto articolo prevede che tali dati siano trattati secondo il principio di lealtà, per finalità determinate e garantisce a ogni persona il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica. Esso stabilisce, inoltre, che il rispetto di tale diritto è soggetto al controllo di un'autorità indipendente. L'articolo 47 garantisce il diritto a un ricorso effettivo nonché il diritto a che la causa sia esaminata equamente, pubblicamente ed entro un termine ragionevole.*

Iniziando a pubblicare, nel giugno 2013, i « documenti Snowden », i media di tutto il mondo hanno portato alla luce l'esistenza di ampi programmi di sorveglianza globale da parte dei servizi di intelligence. Le rivelazioni di Snowden non sono state le prime a suggerire l'esistenza di programmi di sorveglianza delle comunicazioni su vasta scala in seguito agli attentati dell'11 settembre 2001. L'entità di tali rivelazioni, tuttavia, rimane senza precedenti, con potenziali ripercussioni sulla vita privata delle persone in tutto il mondo. La sorveglianza non si limita più soltanto ai segreti di Stato o commerciali, ma permette l'intercettazione delle comunicazioni delle persone su vasta scala. Questo interferisce sia con il rispetto della vita privata e familiare degli individui, sia con il diritto alla vita privata e alla protezione dei dati – entrambi tutelati a livello europeo dalla

Carta dei diritti fondamentali dell'Unione europea (la Carta). Pertanto, l'Unione europea e i suoi Stati membri hanno l'obbligo di tutelarli anche nel contesto della sorveglianza e di fornire alle vittime mezzi di ricorso atti a contestare la sorveglianza illegale.

*« Una siffatta sorveglianza massiccia e indifferenziata è sproporzionata per natura e costituisce un'ingerenza ingiustificata nei diritti garantiti dagli articoli 7 e 8 della Carta »*

(CGUE, C-362/14, Maximilian Schrems contro Data Protection Commissioner, conclusioni dell'avvocato generale, 23 settembre 2015)

Le rivelazioni hanno innescato una serie di reazioni. Nel campo dell'intelligence, e in particolare tra gli organismi specializzati responsabili del controllo dei servizi di intelligence, inchieste dedicate e relazioni speciali sulle rivelazioni di Snowden ne hanno ulteriormente analizzato le implicazioni. Le istituzioni europee hanno reagito con fermezza. La Commissione europea, il Consiglio dell'Unione europea e il Parlamento europeo hanno riferito in merito alle rivelazioni, manifestato preoccupazione per i programmi di sorveglianza di massa, chiesto chiarimenti alle autorità statunitensi e si sono impegnati a « ricostruire la fiducia » nei rapporti USA-UE. Sebbene sia troppo presto per valutare le ripercussioni complessive delle rivelazioni di Snowden, le inchieste post-Snowden condotte in alcuni Stati membri dell'Unione europea hanno portato a concludere che gli attuali quadri giuridici nazionali richiedono una riforma. Ciò è stato ulteriormente sottolineato dalla risoluzione del Parlamento europeo del marzo 2014 sul programma di sorveglianza dell'Agenzia

nazionale per la sicurezza (NSA) degli Stati Uniti, sugli organi di sorveglianza in diversi Stati membri e sul loro impatto sui diritti fondamentali dei cittadini dell'UE nonché sulla cooperazione transatlantica nel campo della giustizia e degli affari interni (2013/2188(INI), P7\_TA (2014) 0230), che vara un *Habeas Corpus digitale europeo*.

« *Le rivelazioni di Snowden ci hanno dato la possibilità di reagire. Spero che trasformeremo quelle reazioni in qualcosa di positivo e duraturo nel prossimo mandato del Parlamento, in una legislazione sulla protezione dei dati di cui tutti possiamo essere orgogliosi* »

(Claude Moraes, eurodeputato, relatore nell'inchiesta del Parlamento europeo sulla NSA, comunicato stampa, 12 marzo 2014)

## Mappatura dei quadri giuridici degli Stati membri in materia di sorveglianza

Nell'aprile 2014, il Parlamento europeo ha chiesto all'Agenzia dell'Unione europea per i diritti fondamentali (FRA) di « effettuare una ricerca approfondita sulla tutela dei diritti fondamentali nel contesto della sorveglianza ». La FRA vi ha provveduto, delineando i quadri giuridici dei ventotto Stati membri dell'UE in materia di sorveglianza e fornendo una panoramica delle norme vigenti sui diritti fondamentali. Inoltre, ha analizzato nei dettagli i meccanismi di controllo e i mezzi di ricorso a disposizione delle persone che riferiscono violazioni del loro diritto alla vita privata.

La ricerca giuridica della FRA non esamina le tecniche di sorveglianza in quanto tali, bensì analizza il modo in cui i quadri giuridici attuali consentono l'uso di tali tecniche ed esamina il ruolo fondamentale svolto dagli organismi specializzati nella vigilanza dell'operato dei servizi di intelligence. Analizza, inoltre, la misura in cui le pertinenti misure di

garanzia tutelano la vita privata e proteggono i dati nei ventotto Stati membri dell'UE.

I « servizi di intelligence » agiscono su mandato estero e si concentrano sulle minacce esterne, mentre i « servizi di sicurezza » agiscono su mandato nazionale e si occupano delle minacce interne. La relazione della FRA utilizza « servizi di intelligence » come termine generico per riferirsi a entrambi.

Questa sintesi presenta i risultati principali della ricerca condotta dalla FRA, che sono pubblicati per esteso nella relazione intitolata *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU – Mapping Member States' legal frameworks* (Sorveglianza da parte dei servizi di intelligence: garanzie dei diritti fondamentali e mezzi di ricorso nell'Unione europea - Mappatura dei quadri giuridici degli Stati membri) (cfr. Ulteriori informazioni).

### Raccolta dei dati e oggetto d'indagine

Ai fini della presente ricerca, la FRA ha esaminato il quadro giuridico in materia di sorveglianza nei ventotto Stati membri dell'UE, analizzando le leggi e le pertinenti norme di tutela dei diritti fondamentali, per presentare una ricerca comparativa del contesto normativo in cui è esercitata detta sorveglianza in tutta l'Unione europea.

Sulla base delle risposte fornite dalla Franet, la rete di ricerca multidisciplinare dell'Agenzia, quest'ultima ha raccolto dati e informazioni attraverso

una ricerca documentaria condotta in tutti i ventotto Stati membri dell'UE. Ulteriori informazioni sono state raccolte attraverso scambi con i partner chiave, tra cui un certo numero di funzionari di collegamento nazionali della FRA negli Stati membri, organismi specializzati ed esperti indipendenti. I risultati si basano anche su relazioni e pubblicazioni esistenti, volte ad assistere i legislatori nazionali nella realizzazione di quadri giuridici per i servizi di intelligence e il loro controllo democratico.

Una seconda relazione socio-legale con i pareri della FRA, basata su una ricerca empirica, sarà pubblicata in una fase successiva, ampliando ulteriormente i risultati qui presentati.

# Garanzie dei diritti fondamentali e diritto dell'UE

« *L'amara verità è che l'uso delle tecnologie di sorveglianza di massa abolisce di fatto il diritto alla riservatezza delle comunicazioni in Internet* »

(*Relatore speciale delle Nazioni Unite sulla promozione e la protezione dei diritti umani e delle libertà fondamentali nella lotta contro il terrorismo*, quarta relazione annuale presentata all'Assemblea Generale, A/69/397, 23 settembre 2014)

Gli Stati membri dell'UE sono tutti vincolati da norme minime di diritto internazionale in materia di diritti umani elaborate dalle Nazioni Unite (ONU), che sono di applicazione universale, come la Human Rights Council Resolution on the right to privacy in the digital age (Risoluzione del Consiglio dei diritti dell'uomo sul diritto alla privacy nell'era digitale, doc. A/HRC/28/L.27, 24 marzo 2015). Diversi organismi specializzati e organi istituiti da trattati delle Nazioni Unite hanno condannato le pratiche di sorveglianza di massa a seguito delle rivelazioni di Snowden. Anche le normative del Consiglio d'Europa, compresa la giurisprudenza della Corte europea dei diritti dell'uomo (Corte EDU), delineano norme minime. Inoltre, è rilevante il diritto dell'UE come interpretato dalla Corte di giustizia dell'Unione europea (CGUE). Infine, in un settore in cui sono direttamente applicabili solo un numero limitato di normative internazionali – oltre alla legislazione internazionale esistente in materia di diritti umani – anche le misure di autoregolamentazione e le norme non vincolanti sono importanti.

La relazione verte sui diritti alla vita privata e alla protezione dei dati, che sono sanciti dagli articoli 7 e 8 della Carta. Il diritto alla protezione dei dati è enunciato anche nel diritto primario e derivato dell'UE, i quali garantiscono, nei loro rispettivi ambiti di applicazione, che il trattamento dei dati personali sia effettuato in modo lecito e solo nella misura necessaria per raggiungere lo scopo legittimamente perseguito. Tali diritti si estendono a tutte le persone, siano essi cittadini dell'UE o di paesi terzi. Ai sensi dell'articolo 52, paragrafo 1, della Carta, eventuali limitazioni all'esercizio di tali diritti devono essere necessarie e proporzionali, rispondere effettivamente a finalità di interesse generale riconosciute dall'Unione, essere previste dalla legge e rispettare il contenuto essenziale di detti diritti.

Nonostante l'esistenza di orientamenti internazionali, manca un'interpretazione univoca della nozione di « sicurezza nazionale » nell'UE. Né la legislazione dell'UE né la giurisprudenza della CGUE definiscono ulteriormente tale nozione, sebbene la CGUE abbia affermato che le eccezioni ai diritti fondamentali

devono essere interpretate in maniera restrittiva e giustificata.

Tale definizione poco chiara di « sicurezza nazionale » si ripercuote sull'applicabilità del diritto dell'UE. L'articolo 4, paragrafo 2, del trattato sull'Unione europea stabilisce che « la sicurezza nazionale resta di esclusiva competenza di ciascuno Stato membro ». Questo non significa che la deroga della « sicurezza nazionale » renda il diritto dell'Unione del tutto inapplicabile. Sono infatti le istituzioni dell'UE, e segnatamente la CGUE, ad avere la facoltà di valutare l'interpretazione di « sicurezza nazionale » a livello degli Stati membri e il modo in cui i programmi di sorveglianza sono realizzati.

## Tipi di sorveglianza: mirata e non mirata

Lo studio condotto dalla FRA esamina come la sorveglianza mirata e non mirata sono organizzate nell'ambito dei quadri giuridici degli Stati membri dell'UE.

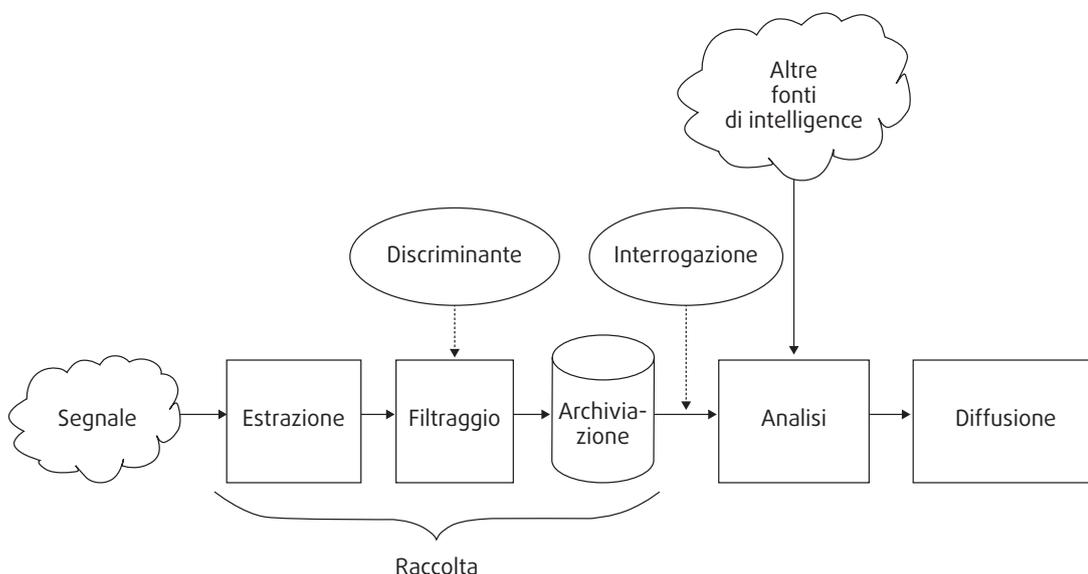
Il comitato di sorveglianza dei servizi di intelligence e sicurezza (CTIVD) dei Paesi Bassi definisce la sorveglianza mirata e non mirata come segue:

- l'intercettazione mirata si riferisce « [all'] intercettazione nella quale la persona, l'organizzazione o la caratteristica tecnica cui la raccolta dei dati è mirata possono essere specificate preventivamente »;
- l'intercettazione non mirata si riferisce « [all'] intercettazione nella quale la persona, l'organizzazione o la caratteristica tecnica cui la raccolta dei dati è mirata non possono essere specificate preventivamente ».

CTIVD, *Relazione annuale 2013-2014*, L'Aia, 31 marzo 2014, pagg. 45-46

La portata dei dati raccolti attraverso i programmi di sorveglianza rivelati – come PRISM, Xkeyscore e Upstream – ha suscitato ampie reazioni. La « sorveglianza di massa » (spesso intesa come non mirata) comporta la raccolta di una quantità di dati molto diversa rispetto ai metodi tradizionali di sorveglianza segreta (mirata), come il ricorso alle intercettazioni telefoniche, che si fonda su sospetti preesistenti con

**Figura: modello concettuale di intelligence dei segnali**



Fonte: National Research Council (Consiglio nazionale delle ricerche) degli Stati Uniti (2015), pag. 28

riferimento a un individuo o organizzazione determinati. Questo tipo di sorveglianza è comunemente ammessa dalle leggi degli Stati membri dell'UE, mentre la maggior parte dei quadri giuridici di detti Stati membri non disciplina né fa alcun riferimento alla « sorveglianza di massa » in quanto tale. Solo pochi Stati membri dell'UE dispongono di una legislazione dettagliata sull'intelligence dei segnali (SIGINT), che è il termine generico usato per descrivere l'intercettazione di segnali provenienti da fonti diverse dei servizi di intelligence. La ricerca della FRA utilizza il termine « intelligence dei segnali » in tutta la sua analisi.

Il SIGINT deriva dall'intelligence militare. Si riferisce alla raccolta automatizzata di informazioni attraverso l'intercettazione e la raccolta di dati digitali relativi alle attività di intelligence. La figura evidenzia come i segnali raccolti vengono filtrati utilizzando discriminanti o selettori, ossia una serie di parametri inseriti nel processo di filtraggio, a priori o in modalità dinamica, per definire i criteri che determineranno quali dati memorizzare in modo da ottenere le informazioni rilevanti (ad esempio, « tutti gli indirizzi e-mail utilizzati nelle comunicazioni con lo Yemen »).

Il Consiglio nazionale delle ricerche delle Accademie nazionali statunitensi ha fatto riferimento all'intelligence dei segnali come termine comprendente tutti i dati memorizzati su un dispositivo elettronico. La Commissione di Venezia utilizza SIGINT come termine collettivo per indicare gli strumenti e i metodi per intercettare e analizzare le comunicazioni radio (compresi telefoni satellitari e cellulari) e via cavo.

L'analisi della FRA sui quadri giuridici che disciplinano i metodi di sorveglianza dei servizi di intelligence rivela che le legislazioni di cinque Stati membri dell'UE (Francia, Germania, Paesi Bassi, Svezia e Regno Unito) specificano nei dettagli le condizioni che permettono la sorveglianza mirata e non mirata, come l'intelligence dei segnali. Le legislazioni di altri Stati membri specificano tali condizioni in maniera insufficiente, ostacolando un'analisi giuridica delle procedure specifiche in vigore sulla raccolta di intelligence dei segnali. Sebbene le leggi in tali paesi non menzionino specificamente il SIGINT, tale pratica è comunque consentita. Tuttavia, poiché in tali paesi essa è prevista solo in misure di regolamentazione non pubblicate, un'analisi dei quadri giuridici applicabili non sarebbe in grado di fare luce sulla questione.

# Risultati principali

## Servizi di intelligence e leggi sulla sorveglianza

### Obiettivo e struttura dei servizi di intelligence

L'obiettivo principale dei servizi di intelligence nelle società democratiche è quello di proteggere la sicurezza nazionale e i valori fondamentali di una società aperta, utilizzando gli strumenti dei servizi di intelligence. L'organizzazione della comunità di intelligence nei singoli Stati membri dell'UE è strettamente legata agli sviluppi storici specifici del paese e non rispetta necessariamente le norme di tutela dei diritti fondamentali. Di conseguenza, i servizi di intelligence sono organizzati in modi estremamente diversi all'interno dell'UE. In alcuni Stati membri il compito è svolto da due servizi di intelligence, mentre in altri è affidato a cinque o sei organismi.

- Quasi tutti gli Stati membri dell'UE hanno istituito almeno due diversi organismi di intelligence, uno per le questioni civili e l'altro per le questioni militari; queste ultime non sono prese in considerazione nella presente relazione. I servizi di intelligence civili sono generalmente subordinati ai ministeri degli interni, e, talvolta, anche al primo ministro o al presidente.
- In alcuni Stati membri, i servizi civili sono ulteriormente suddivisi in un servizio con un mandato nazionale e un servizio con un mandato estero. Inoltre, alcuni Stati membri hanno affidato le misure di intelligence a unità specializzate in una determinata minaccia, come la criminalità organizzata, la corruzione o la lotta contro il terrorismo.

### Protezione della sicurezza nazionale

Lo studio condotto dalla FRA esamina il concetto di « sicurezza nazionale » alla luce del mandato dei servizi di intelligence e delle misure di sorveglianza che essi possono attuare. Anche in questo caso, i risultati rivelano notevoli differenze tra gli Stati membri dell'UE.

- L'obiettivo principale dei servizi di intelligence è quello di proteggere la sicurezza nazionale, ma il concetto non è armonizzato in tutti gli Stati membri dell'UE. La portata della sicurezza

nazionale è raramente definita e talvolta vengono utilizzati termini simili. Altri Stati membri non usano affatto il termine « sicurezza nazionale » e fanno invece riferimento alla « sicurezza interna » e/o alla « sicurezza esterna », o alla « sicurezza dello Stato ».

- L'ambito dei diversi compiti dei servizi di intelligence (cioè il loro mandato) non è identico in tutti gli Stati membri dell'UE. Oltre ai settori più tradizionali, i mandati di alcuni servizi di intelligence includono la criminalità organizzata e la criminalità informatica. Questi termini non sono definiti in modo armonizzato.

### Regolamentazione giuridica della sorveglianza

La linea di demarcazione tra i compiti delle forze dell'ordine e quelli dei servizi di intelligence non è sempre netta. Ogni ampliamento dei compiti deve essere opportunamente giustificato come necessario per la salvaguardia dello Stato, che è la ragione sottesa all'istituzione dei servizi di intelligence.

- I quadri giuridici della maggior parte degli Stati membri disciplinano solo la sorveglianza mirata di individui o gruppi/organizzazioni definiti. Oltre a prevedere la sorveglianza mirata, cinque Stati membri hanno promulgato leggi dettagliate sulle condizioni per l'utilizzo dell'intelligence dei segnali.
- Guardando alle norme applicabili sui diritti umani, i quadri giuridici nazionali mancano di definizioni chiare, che indichino le categorie di persone e l'ambito delle attività che possono essere soggette alla raccolta di dati di intelligence.
- Nella maggior parte degli Stati membri (ventisei su ventotto), i servizi di intelligence sono disciplinati dalla legge per mezzo di disposizioni in materia di organizzazione e funzionamento degli stessi. La costituzione di uno Stato membro vieta al proprio servizio di intelligence di svolgere compiti di sorveglianza. Un altro Stato membro è in procinto di promulgare una legislazione che regolamenti le pratiche di sorveglianza dei propri servizi di intelligence.
- L'analisi della FRA mostra che la base giuridica su cui si fondano i mandati e i poteri dei servizi nazionali di intelligence negli Stati membri dell'UE va da un unico atto legale che disciplina l'organizzazione e gli strumenti di tali servizi fino

a quadri complessi che consistono di diverse leggi e ordinanze atte a regolamentare aspetti specifici dei relativi mandati, organizzazione, competenze o strumenti.

- La maggior parte degli Stati membri organizza il lavoro dei servizi di intelligence in due leggi: una verte sul mandato e l'organizzazione del servizio, l'altra sugli strumenti di azione e le condizioni per il loro utilizzo.
- La maggior parte degli Stati membri dell'UE (ventitré su ventotto) dispone di servizi di intelligence separati dalle autorità preposte all'applicazione della legge. Due Stati membri si sono recentemente discostati da sistemi in cui i servizi di intelligence appartenevano alla polizia o ad altre autorità preposte all'applicazione della legge.

## Controllo dei servizi di intelligence

L'analisi della FRA esamina i meccanismi di responsabilità in materia di sorveglianza da parte dei servizi di intelligence. Essa descrive, in particolare, come gli Stati membri dell'UE hanno istituito i meccanismi di controllo. Il controllo è un mezzo per garantire la responsabilità pubblica per le decisioni e le azioni dei servizi di intelligence. Secondo gli esperti, il controllo mira a evitare l'abuso di potere, legittimare l'esercizio di poteri invasivi e ottenere migliori risultati in seguito alla valutazione di azioni specifiche. Secondo l'opinione generale che emerge da una relazione della Commissione di Venezia e da altri studi accademici, la sorveglianza dovrebbe essere una combinazione tra:

- controllo da parte dell'esecutivo,
- controllo parlamentare,
- controllo da parte di organismi di esperti,
- controllo giurisdizionale.

## Controllo da parte dell'esecutivo e coordinamento tra gli organismi di controllo

L'esecutivo può controllare i servizi di intelligence in diversi modi: specificandone le politiche strategiche e le priorità o definendo orientamenti; nominando e/o designando gli alti dirigenti del servizio; formulando il bilancio, che sarà comunque votato dal Parlamento; o approvando la collaborazione con

altri servizi. L'esecutivo riveste un ruolo fondamentale anche nell'autorizzare le misure di sorveglianza in taluni Stati membri.

Un controllo efficace richiede un adeguato coordinamento tra i vari organismi di controllo, per garantire che ogni aspetto del lavoro dei servizi di intelligence sia coperto. Se gli organismi di controllo non hanno una conoscenza chiara e globale del lavoro di tutto il settore nazionale dell'intelligence, il controllo risulterà lacunoso e l'efficacia del sistema di controllo nel suo complesso ne sarà sminuita.

- La diversità tra gli Stati membri dell'UE in termini di politica e sistemi giuridici si è tradotta in una grande varietà di organismi che sorvegliano i servizi di intelligence. Gli Stati membri dell'UE dispongono di sistemi di controllo estremamente diversi. Se da una parte dai sistemi in vigore si possono desumere buone prassi, dall'altra vi sono singoli settori che trarrebbero beneficio da una riforma giuridica volta a rafforzare il potere degli organismi di controllo.
- Ai diversi organismi di controllo sono conferiti una grande varietà di poteri, con facoltà di esercitarli in misure diverse.
- Sette Stati membri dispongono di sistemi di controllo che combinano l'esecutivo, il parlamento, la magistratura (mediante approvazione ex-ante) e organismi di esperti. Tuttavia, tra questi non vi è nessuno dei paesi dotati di quadri giuridici che prevedono la raccolta di dati di intelligence dei segnali.
- Un controllo efficace non richiede necessariamente tutti e quattro i tipi di meccanismi di controllo. Tale controllo può essere effettuato a condizione che gli organismi previsti si complementino a vicenda e che nel complesso costituiscono un sistema efficace, atto a valutare se il mandato dei servizi di intelligence sia eseguito in modo appropriato. Ciò si verifica se i poteri di controllo coprono tutti i settori di attività di un servizio di intelligence. Qualora il mandato in sé non sia chiaro o sia insufficientemente sviluppato, tuttavia, gli organismi di controllo non saranno in grado di esercitare alcuna influenza.
- L'accesso alle informazioni e ai documenti da parte degli organismi di controllo è essenziale. Mentre le informazioni raccolte dai servizi di intelligence sono sensibili e le misure di salvaguardia devono garantire che esse siano trattate di conseguenza, gli organismi di controllo non possono svolgere i propri compiti senza avere accesso a tutte le informazioni pertinenti. Il contrario, tuttavia, sembra essere la norma.

## Controllo parlamentare

Il controllo parlamentare è importante, data la responsabilità del Parlamento nell'attribuire responsabilità al governo. Il Parlamento, in quanto legislatore, è responsabile dell'emanazione di una legislazione chiara e accessibile, che istituisce i servizi di intelligence e ne definisce organizzazione, poteri speciali e limitazioni. È inoltre incaricato dell'approvazione del bilancio dei servizi di intelligence e, in alcuni Stati membri, verifica se le loro attività sono in linea con il quadro giuridico.

- I risultati della FRA mostrano che ventiquattro Stati membri dell'UE prevedono un controllo parlamentare; in ventuno di questi, i servizi di intelligence sono controllati da commissioni parlamentari speciali. Alcuni Stati membri hanno istituito un'unica commissione parlamentare che si occupa dei diversi servizi di sicurezza e di intelligence, mentre altri hanno creato diverse commissioni che si occupano dei servizi individualmente.
- A nessuna commissione parlamentare di uno Stato membro è concesso accesso illimitato ai dati di intelligence.
- Le diverse commissioni parlamentari degli Stati membri hanno mandati differenti: la maggior parte dispone di poteri di controllo tradizionali legati alla legislazione, al bilancio e al ricevimento delle informazioni sulla funzione dei servizi, mentre poche possono gestire i ricorsi, prendere decisioni vincolanti concernenti i servizi di intelligence o assistere nell'approvazione di misure di sorveglianza.
- In termini del potere delle commissioni parlamentari di avviare inchieste, le legislazioni della maggior parte dei paesi autorizzano tali commissioni a richiedere informazioni ai servizi di intelligence o all'esecutivo, ma non a esigerle.

## Controllo da parte di organismi di esperti

Il controllo da parte di esperti è particolarmente prezioso, dal momento che consente a persone che hanno familiarità con la materia, tempo di dedicarsi alla questione e sono indipendenti da alleanze politiche di monitorare le azioni dei servizi di intelligence. Secondo il Commissario per i diritti umani del Consiglio d'Europa, essi sono spesso nella posizione migliore per effettuare controlli quotidiani sulle attività dei servizi di sicurezza e di intelligence.

- Anche se il controllo parlamentare è fondamentale, esso deve essere integrato da altri

organismi di controllo, in particolare da efficaci organismi di esperti, che possono controllare le attività operative, compresi la raccolta, lo scambio e l'utilizzo di dati personali nonché la tutela del diritto alla vita privata.

- Nell'UE, quindici Stati membri hanno istituito uno o più organismi di esperti dedicati esclusivamente al controllo dei servizi di intelligence. Le loro competenze includono l'autorizzazione delle misure di sorveglianza, l'esame dei ricorsi, la richiesta di documenti e informazioni ai servizi di intelligence e la consulenza fornita all'esecutivo e/o al Parlamento. Affinché possano sfruttare al massimo il loro potenziale, devono essere loro concessi indipendenza, risorse e poteri adeguati.
- In alcuni Stati membri, l'autorizzazione delle misure di sorveglianza non coinvolge alcuna istituzione indipendente dai servizi di intelligence e dall'esecutivo.
- Negli Stati membri che dispongono di un organismo indipendente incaricato di autorizzare le misure di sorveglianza, la sorveglianza mirata richiede tendenzialmente l'approvazione giudiziaria, mentre l'approvazione di organismi di esperti è l'altra soluzione preferita. Non esiste un approccio comune al controllo della raccolta di dati di intelligence dei segnali.
- Se la conoscenza degli aspetti giuridici della sorveglianza è indispensabile, gli organismi di esperti devono anche essere tecnicamente competenti. Alcuni Stati membri perseguono tale obiettivo integrando esperti provenienti da diversi settori, tra cui le tecnologie dell'informazione e delle comunicazioni (TIC). Altri fanno grande affidamento su una combinazione di giudici e parlamentari, ancora in carica o no.

Negli Stati membri dell'UE, alle autorità di protezione dei dati (DPA) – organismi specializzati chiamati a salvaguardare la privacy e la protezione dei dati – è stato assegnato un ruolo fondamentale nella protezione dei dati personali. Questo ruolo è sancito dal diritto primario e secondario dell'UE. Ma gli organismi di esperti specializzati nel controllo dei servizi di intelligence dispongono, senza dubbio, di competenze riconosciute nella tutela dei dati e della privacy nel settore dell'intelligence.

- I risultati della FRA mostrano che, rispetto ad altre attività di trattamento dei dati e ad altri responsabili del trattamento dei dati nel settore pubblico e privato, in sette Stati membri le DPA dispongono, nei confronti dei servizi di intelligence, degli stessi poteri attribuiti a tutti gli altri responsabili del trattamento dei dati. In dodici Stati membri, le DPA non hanno alcuna

competenza rispetto ai servizi di intelligence e in nove di essi i loro poteri sono limitati.

- Negli Stati membri in cui le DPA e altri organismi specializzati di controllo condividono le competenze, una mancanza di cooperazione tra essi può risultare in lacune, derivanti dalla frammentazione delle responsabilità. Negli Stati membri in cui le DPA non hanno competenza sui servizi di intelligence, l'organismo di controllo è responsabile di assicurare la corretta applicazione delle misure per la tutela della vita privata e la protezione dei dati.
- Uno studio precedente condotto dalla FRA nel settore dell'accesso ai mezzi di ricorso per la protezione dei dati individua l'esigenza di migliorare le capacità delle DPA; ciò è importante in considerazione del ruolo che queste potrebbero rivestire nella supervisione dei servizi di intelligence.

## Mezzi di ricorso

In base alle norme internazionali applicabili, chiunque si ritenga vittima di una violazione della privacy o della protezione dei dati deve avere la possibilità di esperire mezzi di ricorso per porre rimedio alla situazione. Il diritto a un ricorso effettivo – che consente alle persone di far valere una violazione dei propri diritti – è una componente essenziale dell'accesso alla giustizia. Un ricorso deve essere « effettivo » de facto e de iure.

Come mostrano precedenti relazioni della FRA sull'accesso ai mezzi di ricorso per la protezione dei dati e l'accesso alla giustizia, una serie di percorsi correttivi sono a disposizione delle vittime di violazioni della privacy e della protezione dei dati. Gli organi extragiudiziali rivestono un ruolo correttivo importante nel settore della sorveglianza, tenuto conto delle difficoltà pratiche di accesso ai tribunali. Gli organi non giudiziari dei ventotto Stati membri dell'UE includono organismi di esperti (comprese le DPA), esecutivi e parlamentari, come pure le istituzioni dei difensori civici. In alcuni Stati membri, il numero di organismi extragiudiziali con ruoli correttivi nel settore della sorveglianza è relativamente incoraggiante, ma deve essere considerato alla luce dei risultati indicati di seguito.

La complessità del panorama correttivo non facilita l'attuazione di misure correttive efficaci, né facilita la quantità di dati raccolti dai servizi di intelligence che utilizzano il SIGINT. La frammentazione e la compartimentalizzazione dei diversi percorsi correttivi hanno reso difficile esperire mezzi di ricorso. Di fatto, dai dati raccolti emerge che solo un numero limitato di controversie concernenti prassi di sorveglianza è stato giudicato a livello nazionale dopo le rivelazioni di Snowden.

## Obbligo d'informazione e diritto di accesso

Il diritto a essere informati e ad accedere alle informazioni è fondamentale per segnalare alle persone le misure di sorveglianza e avviare un'azione correttiva. La Corte europea dei diritti dell'uomo (Corte EDU) ha, tuttavia, accettato che tali diritti possano ragionevolmente essere limitati (cfr. Corte EDU, *Klass et al. c. Germania*, n. 5029/71, 6 settembre 1978). I risultati della FRA mostrano che la segretezza intorno al lavoro dei servizi di intelligence limita, di fatto, tali diritti. Un altro fattore è costituito dall'eccezionale quantità di dati raccolti attraverso il SIGINT rispetto a forme più tradizionali di sorveglianza.

- In otto Stati membri, l'obbligo d'informazione e il diritto di accesso non sono affatto previsti dalla legge; si applicano le norme relative ai documenti classificati o a segreti ufficiali. Negli altri venti Stati membri, la legislazione prevede l'obbligo di informazione e il diritto di accesso, in alcuni casi entro un certo termine, ma con restrizioni. Tali restrizioni includono diversi motivi, come la sicurezza nazionale, gli interessi nazionali o lo scopo della misura di sorveglianza stessa.
- Solo due Stati membri prevedono disposizioni specifiche in merito all'obbligo d'informazione nel contesto dell'intelligence dei segnali: nel primo, gli individui non sono informati se i selectori utilizzati non sono direttamente attribuibili all'individuo; nell'altro, l'individuo non è informato se i dati personali acquisiti vengono cancellati immediatamente dopo la raccolta, senza essere trattati ulteriormente.
- Gli organi di controllo di dieci Stati membri dell'UE, tra cui sei DPA nazionali, verificano le restrizioni del diritto a essere informati e del diritto di accesso alle informazioni, controllando se la presunta minaccia alla sicurezza nazionale sia ragionevole e/o esercitando indirettamente il diritto di accesso della persona. In quest'ultimo caso, gli organismi valutano se l'accesso ai dati può essere autorizzato o se il rifiuto è legittimo e verificano inoltre la legittimità del trattamento dei dati. In uno Stato membro, è necessaria un'ingiunzione del tribunale, attestante che la notificazione comprometterebbe l'indagine o che vi sono altri argomenti a sfavore.
- Due altri Stati membri non concedono il diritto di accesso alle informazioni in quanto tale. La legge, tuttavia, prevede un diritto che produce lo stesso risultato: una persona può chiedere all'organismo di controllo di verificare se i suoi dati sono oggetto di sorveglianza illegale.

- In alcuni Stati membri, l'organo di controllo che esercita indirettamente il diritto individuale di richiedere l'accesso ai dati non conferma né nega il trattamento dei dati. Le risposte si limitano, in genere, a dichiarare che il ricorso è stato gestito e/o controllato.

## Mezzi di ricorso giurisdizionali

Ogni Stato membro offre alle persone la possibilità di agire per via giudiziaria in caso di violazione della privacy, indipendentemente dal fatto che essa sia verificata in conseguenza di intelligence mirata o intelligence dei segnali. I tribunali offrono alle persone un canale per presentare ricorso in caso di interferenza nella loro vita privata, comprese le impugnazioni delle decisioni dell'organismo di controllo in merito alle loro denunce di violazione della privacy. Offrono inoltre alle persone l'opportunità di esperire mezzi di ricorso, anche nel settore della sorveglianza.

- Uno studio condotto dalla FRA ha tuttavia individuato la mancanza di specializzazione dei giudici in materia di protezione dei dati come un serio ostacolo per rimediare efficacemente alle violazioni della protezione dei dati. Questa scoperta è rilevante per la sorveglianza dove, oltre alla necessaria segretezza legata all'intelligence, competenze specifiche nel campo delle TIC o dell'intelligence, ad esempio, sono essenziali.
- Solo due Stati membri hanno rimediato alla mancanza di specializzazione con riferimento ai mezzi di ricorso, coinvolgendo giudici/tribunali che dispongono delle conoscenze necessarie per decidere su questioni (spesso) tecniche e che sono autorizzati ad accedere a materiale segreto.

## Mezzi di ricorso extragiudiziali

Le opzioni extragiudiziali sono solitamente più accessibili alle persone rispetto ai meccanismi giudiziari perché le norme procedurali sono meno severe, presentare ricorsi è meno dispendioso e i procedimenti sono più rapidi. Ciò è confermato da prove precedentemente fornite dalla FRA, segnatamente nel contesto della protezione dei dati, dato che un maggior numero di ricorsi tende a essere presentato presso le DPA nazionali, mentre solo pochi denunciatori avviano procedimenti giudiziari. Il numero di organismi extragiudiziali – diversi dalle DPA – che operano nel settore della protezione dei dati è tuttavia ridotto e molti di tali organismi dispongono solo di un potere limitato di offrire ricorsi.

- Gli organismi di controllo (tra cui le DPA) incaricati del trattamento dei ricorsi sono istituzioni indipendenti nella maggior parte degli Stati membri.

- Quando un organismo di controllo esecutivo dispone di poteri correttivi, la questione dell'indipendenza si pone quando esso dispone anche del potere di garantire la sorveglianza. Gli organismi di controllo parlamentari e di esperti dispongono di strutture amministrative più autonome – ma l'autonomia non garantisce un ricorso effettivo, a meno che sia accompagnata anche da una conoscenza sufficiente. Il modo in cui i membri degli organismi di controllo vengono designati e il posto che occupano nella gerarchia amministrativa sono aspetti altrettanto importanti da considerare quando si valuta l'indipendenza di un organismo.

- Le DPA in tredici Stati membri dell'UE hanno il potere di esaminare singoli ricorsi ed emanare decisioni vincolanti. In tre di questi, tuttavia, il potere di accedere ad archivi e locali è limitato. In cinque Stati membri si applicano ulteriori requisiti, che impongono la presenza del capo o di un membro della DPA durante le ispezioni presso i locali del servizio di intelligence.

- Su sette Stati membri che conferiscono ai loro organismi di controllo di esperti (diversi dalle DPA) specifici poteri correttivi, cinque permettono anche a tali organismi di emettere decisioni vincolanti. In due Stati membri dell'UE, un organo di controllo esecutivo dispone anche di poteri correttivi. Le commissioni parlamentari in quattro Stati membri hanno il diritto di accogliere ricorsi individuali, ma solo una di esse può risolverli con decisioni vincolanti.

- La figura del difensore civico, che esiste in tutti i ventotto Stati membri dell'UE, si occupa essenzialmente di inadempienze amministrative, piuttosto che dei meriti specifici della sorveglianza. Un solo Stato membro conferisce poteri correttivi al difensore civico attraverso la pertinente legge sull'intelligence. Inoltre, i poteri del difensore civico possono essere alquanto limitati e i procedimenti si concludono, in genere, con raccomandazioni non vincolanti, che mirano a risolvere le situazioni e orientare le azioni future, piuttosto che con una sentenza esecutiva vincolante. Ciò influisce, ovviamente, sull'efficacia dei rimedi che sono in grado di fornire.

- Altri elementi che possono facilitare l'accesso di una persona ai mezzi di ricorso comprendono norme più flessibili sull'onere probatorio e le *class action* (azioni collettive), nonché un'efficace protezione degli informatori. L'Assemblea parlamentare del Consiglio d'Europa considera la denuncia di irregolarità lo strumento più efficace per garantire l'osservanza dei limiti posti in materia di sorveglianza.

## Conclusioni

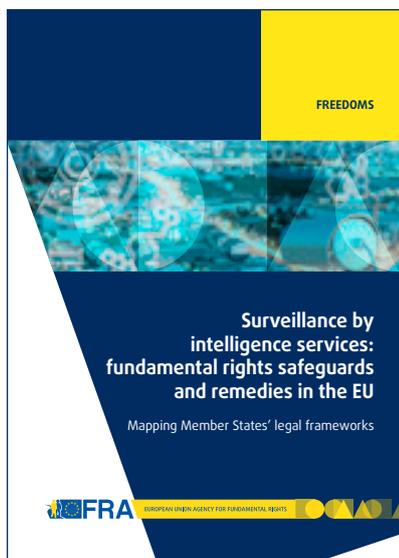
Incentrata su un settore di competenza limitata dell'UE, la relazione sottolinea le diversità tra gli Stati membri per quanto riguarda l'organizzazione dei servizi di intelligence e le modalità di svolgimento dei loro compiti essenziali.

Le misure di sorveglianza interferiscono significativamente con i diritti individuali. Data la loro natura segreta, le persone sono tenute ad avere un certo grado di fiducia nelle autorità pubbliche che, a loro volta, sono tenute a salvaguardare i diritti fondamentali delle persone. Per raggiungere il livello di fiducia che una società deve avere nei confronti del proprio servizio di intelligence, è necessario che siano definite le responsabilità e chi deve farsene carico. Una legislazione chiara e accessibile, meccanismi di controllo efficaci, meccanismi di vigilanza adeguati e mezzi di ricorso efficaci sono solo alcuni degli elementi essenziali per ottenere questo tipo di responsabilizzazione, che resta innegabilmente difficile a causa della segretezza nella quale operano i servizi di intelligence. L'introduzione e il mantenimento di una legislazione chiara e accessibile e di meccanismi di controllo forti a livello degli Stati membri costituisce solo il primo passo verso un sistema trasparente e conforme al rispetto dei diritti fondamentali; tuttavia, le difficoltà nel raggiungimento di tale obiettivo indicano che rimangono degli ostacoli.

Le reazioni alle rivelazioni di Snowden hanno evidenziato la necessità di adattare e rafforzare i pertinenti quadri giuridici nell'UE e in tutti i suoi Stati membri. La ricerca della FRA evidenzia che è già stato attuato un certo numero di riforme giuridiche. Valutazioni periodiche del funzionamento e della legittimità dei quadri giuridici che regolamentano l'attività di intelligence devono diventare parte integrante dei sistemi di controllo. Un'altra questione chiave è il modo in cui riformare ulteriormente i quadri giuridici, per ovviare alla mancanza di un controllo adeguato. Inoltre, le riforme negli Stati membri dell'UE devono tenere conto dei recenti sviluppi tecnologici, al fine di garantire che ai meccanismi di controllo siano forniti i necessari strumenti e conoscenze specialistiche. Il raggiungimento di tutti questi obiettivi è innegabilmente difficile, ma fondamentale per adempiere il difficile compito di proteggere la sicurezza nel rispetto dei diritti fondamentali.







Proteggere la popolazione dalle minacce alla sicurezza e salvaguardare i diritti fondamentali richiede il raggiungimento di un delicato equilibrio. Brutali attacchi terroristici e innovazioni tecnologiche che rendono possibile il monitoraggio su larga scala dei dati relativi alle comunicazioni hanno ulteriormente complicato la questione, suscitando preoccupazioni circa eventuali violazioni dei diritti alla vita privata e alla protezione dei dati nel nome della tutela della sicurezza nazionale. Le rivelazioni di Snowden, che hanno messo a nudo intense e indifferenziate attività di sorveglianza in tutto il mondo, hanno evidenziato la necessità di maggiori garanzie a salvaguardia di tali diritti.

La presente relazione, redatta in risposta alla richiesta del Parlamento europeo di una ricerca approfondita sulla tutela dei diritti fondamentali nel contesto della sorveglianza, delinea e analizza i quadri giuridici in materia di sorveglianza in vigore negli Stati membri dell'UE. Analizzando la cosiddetta « sorveglianza di massa », la relazione descrive inoltre nel dettaglio i meccanismi di controllo introdotti all'interno dell'UE, delinea il lavoro delle entità incaricate di controllare le attività di sorveglianza e presenta i mezzi di ricorso a disposizione delle persone che intendono contestare tale attività di intelligence. Dimostrando i fatti alla base delle complesse considerazioni sollevate, la presente relazione sottolinea la difficoltà di affrontare quelle che spesso sono viste come priorità concorrenti e contribuisce al dibattito sul modo migliore per riconciliarle.

## Ulteriori informazioni:

La relazione integrale della FRA *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU – Mapping Member States' legal frameworks* (Sorveglianza da parte dei servizi di intelligence: garanzie dei diritti fondamentali e mezzi di ricorso nell'Unione europea - Mappatura dei quadri giuridici degli Stati membri) è reperibile al seguente indirizzo: <http://fra.europa.eu/en/publication/2015/surveillance-intelligence-services>

Pubblicazioni della FRA su argomenti correlati:

- FRA-Consiglio d'Europa (2014), *Manuale sul diritto europeo in materia di protezione dei dati*, Lussemburgo, Ufficio delle pubblicazioni, [http://fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-law-2nd-ed\\_it.pdf](http://fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-law-2nd-ed_it.pdf) (disponibile nelle lingue dell'UE)
- FRA (2014), *Access to data protection remedies in EU Member States* (Accesso ai mezzi di ricorso per la protezione dei dati negli Stati membri dell'Unione europea), Lussemburgo, Ufficio delle pubblicazioni, <http://fra.europa.eu/en/publication/2014/access-data-protection-remedies-eu-member-states> e relazione di sintesi <http://fra.europa.eu/en/publication/2014/access-data-protection-remedies-eu-member-states-summary> (disponibile nelle lingue dell'UE)

Una panoramica delle attività della FRA sulla protezione dei dati è disponibile all'indirizzo: <http://fra.europa.eu/en/theme/information-society-privacy-and-data-protection>



Ufficio delle pubblicazioni

FRA – AGENZIA DELL'UNIONE EUROPEA PER I DIRITTI FONDAMENTALI

Schwarzenbergplatz 11 – 1040 Vienna – Austria  
Tel.: +43 158030-0 – Fax: +43 158030-699  
[fra.europa.eu](http://fra.europa.eu) – [info@fra.europa.eu](mailto:info@fra.europa.eu)  
[facebook.com/fundamentalrights](https://www.facebook.com/fundamentalrights)  
[linkedin.com/company/eu-fundamental-rights-agency](https://www.linkedin.com/company/eu-fundamental-rights-agency)  
[twitter.com/EURightsAgency](https://twitter.com/EURightsAgency)



Print: ISBN 978-92-9491-013-4, doi:10.2811/921414  
PDF: ISBN 978-92-9491-039-4, doi:10.2811/092101