Tradotto con Google translator da
https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2020/05/rs20200519_1bvr283517.html

Principi guida sulla sentenza del Primo Senato del 19 maggio 2020

- 1 BvR 2835/17 -

1. Il vincolo dell'autorità statale tedesca ai diritti fondamentali secondo l'articolo 1 capoverso 3 GG non si limita al territorio tedesco.

1. La protezione dei diritti fondamentali individuali può differire in Germania e all'estero.

2. In ogni caso, la protezione dell'Articolo 10 Paragrafo 1 e dell'Articolo 5 Paragrafo 1 Frase 2 GG come diritti di difesa contro la sorveglianza delle telecomunicazioni si estende anche agli stranieri all'estero.

2. Le attuali norme per la sorveglianza delle telecomunicazioni oltremare, per la trasmissione delle conoscenze acquisite in tal modo e per la cooperazione con i servizi di intelligence stranieri violano il requisito di quotazione dell'articolo 19.1 frase 2 della Legge fondamentale; il legislatore deliberatamente non ha considerato i diritti fondamentali interessati, sebbene possano essere applicati anche qui. Inoltre, non soddisfano i requisiti materiali fondamentali dei diritti fondamentali.

3. 10 sec.1 GG protegge la riservatezza della comunicazione individuale in quanto tale. Le persone che sostengono che i loro diritti fondamentali sono stati violati non sono escluse dalla protezione dei diritti fondamentali della Legge fondamentale perché agiscono come funzionari di una persona giuridica straniera.

4. La regolamentazione dell'intelligence straniera rientra negli affari esteri ai sensi dell'articolo 73.1 n. 1 GG. Sulla base di questa competenza, al Servizio di intelligence federale può essere assegnato il compito di fornire al governo federale informazioni sulla politica estera e di sicurezza come compito separato e non operativo, nonché l'individuazione tempestiva di pericoli di una dimensione internazionale dall'estero. Devono esserci pericoli che, per loro natura e peso, possono influenzare la posizione della Repubblica Federale nella comunità internazionale e sono di particolare importanza in termini di politica estera e di sicurezza in questo senso.

5. Il controllo strategico delle telecomunicazioni non è sostanzialmente incompatibile con l'articolo 10.1 della Legge fondamentale. Tuttavia, in quanto autorità occasionale, essenzialmente solo alla fine istruita e limitata, è un'autorità eccezionale che deve rimanere limitata alle informazioni fornite all'estero da un'autorità che non ha poteri operativi ed è giustificata solo dal suo profilo di attività speciale.

3. In base a ciò, in particolare, sono necessarie misure per separare i dati di telecomunicazione di tedeschi e residenti, una limitazione dei dati da raccogliere, la definizione di scopi di sorveglianza qualificati, la strutturazione della sorveglianza sulla base di misure appositamente definite, requisiti speciali per misure di sorveglianza personale mirate, limiti per la conservazione dei dati Dati sul traffico, disposizioni quadro per la valutazione dei

dati, precauzioni per proteggere le relazioni riservate, la garanzia della protezione dell'area centrale e obblighi di cancellazione.

6. La trasmissione di dati personali dalla sorveglianza strategica è consentita solo per la protezione di beni giuridici particolarmente importanti e presuppone una situazione di rischio specifica o un sospetto adeguatamente specificato. Ciò non si applica alle segnalazioni al governo federale, a condizione che vengano utilizzate solo per informazioni politiche e per preparare le decisioni del governo.

4. Die Übermittlung setzt eine förmliche Entscheidung des Bundesnachrichtendienstes voraus und bedarf der Protokollierung unter Nennung der einschlägigen Rechtsgrundlage. Vor der Übermittlung an ausländische Stellen ist eine Vergewisserung über den rechtsstaatlichen Umgang mit den Daten geboten; hierbei bedarf es einer auf die betroffene Person bezogenen Prüfung, wenn es Anhaltspunkte gibt, dass diese durch die Datenübermittlung spezifisch gefährdet werden kann.

7. Regelungen zur Kooperation mit ausländischen Nachrichtendiensten genügen grundrechtlichen Anforderungen nur, wenn sie sicherstellen, dass die rechtsstaatlichen Grenzen durch den gegenseitigen Austausch nicht überspielt werden und die Verantwortung des Bundesnachrichtendienstes für die von ihm erhobenen und ausgewerteten Daten im Kern gewahrt bleibt.

5. Will der Bundesnachrichtendienst von einem Partnerdienst bestimmte Suchbegriffe nutzen, um die Treffer ohne nähere inhaltliche Auswertung automatisiert an diesen zu übermitteln, erfordert dies eine sorgfältige Kontrolle dieser Suchbegriffe sowie der hieran anknüpfenden Trefferfälle. Die bei Auslandsübermittlungen geltenden Vergewisserungspflichten gelten entsprechend. Die gesamthafte Übermittlung von Verkehrsdaten an Partnerdienste setzt einen qualifizierten Aufklärungsbedarf im Hinblick auf eine spezifisch konkretisierte Gefahrenlage voraus. Für den Umgang der Partnerdienste mit den übermittelten Daten sind gehaltvolle Zusagen einzuholen.

8. Die Befugnisse zur strategischen Überwachung, zur Übermittlung der mit ihr gewonnenen Erkenntnisse und zur diesbezüglichen Zusammenarbeit mit ausländischen Diensten sind mit den Anforderungen der Verhältnismäßigkeit nur vereinbar, wenn sie durch eine unabhängige objektivrechtliche Kontrolle flankiert sind. Sie ist als kontinuierliche Rechtskontrolle auszugestalten, die einen umfassenden Kontrollzugriff ermöglicht.

6. Hierfür ist einerseits eine mit abschließenden Entscheidungsbefugnissen verbundene gerichtsähnliche Kontrolle sicherzustellen, der die wesentlichen Verfahrensschritte der strategischen Überwachung unterliegen, sowie anderseits eine administrative Kontrolle, die eigeninitiativ stichprobenmäßig den gesamten Prozess der Überwachung auf seine Rechtmäßigkeit prüfen kann.

7. Il controllo nell'indipendenza istituzionale deve essere garantito. Ciò include il proprio budget, la propria sovranità personale e l'autonomia procedurale. Gli organi di controllo devono essere equipaggiati in termini di personale e materiale in modo che possano svolgere efficacemente i loro compiti. Devono disporre di tutti i poteri necessari per un controllo efficace contro il Servizio di intelligence federale. Bisogna anche prestare attenzione a garantire che il controllo non sia ostacolato dalla "regola di terzi".

Annunciato

il 19 maggio 2020

Langendörfer

Dipendenti collettivi

come dipendente pubblico

l'ufficio

CORTE COSTITUZIONALE FEDERALE

- 1 BvR 2835/17 -

IN NOME DELLE PERSONE

Nel procedimento relativo alla denuncia costituzionale

1. der Reporter sans frontières,
   rappresentato dal Directeur général D…,
2 ° donna io ...,
3 ° del Signore G ...,
4 ° di Lord N ...,
5. del signor Z ...,
6. di Lord O ...,
7. del signor L ...,
8 °. del signor M ...,

- Rappresentante autorizzato:

1. 1. Prof. Dr. Matthias Baker, LL.M.,

2. 2. Avvocato Dr. Bijan Moini -

contro § 6 paragrafi 1, 2, 3 e 6,
§ 7 paragrafo 1,
§ 9 paragrafi 4 e 5,
§ 10 paragrafo 3,
§ 13 paragrafo 4,
Sezione 14 sottosezione 1 frase 1 e sottosezione 2,
§ 15 paragrafo 1,
§ 19 paragrafo 1,
§ 24 paragrafo 1 frase 1, paragrafi 2 e 3

della legge sul servizio di intelligence federale (legge BND) nella versione della legge sull'applicazione delle telecomunicazioni estere-straniere del servizio di intelligence federale del 23 dicembre 2016 (Gazzetta federale I pagina 3346)

la Corte costituzionale federale - Primo Senato -

con la partecipazione dei giudici

Vicepresidente Harbarth,

Masing,

Paolo,

Orso,

Britz,

Ott,

Cristiano,

Radtke

basato sull'audizione del 14 e 15 gennaio 2020

giudizio

riconosciuto per diritto:

1. Sezioni 6, 7, da 13 a 15 del Federal Intelligence Service Act come modificato dalla Legge del Servizio di intelligence federale sull'applicazione delle telecomunicazioni all'estero del 23 dicembre 2016 (Gazzetta federale I pagina 3346), anche nella versione della legge sull'adeguamento della legge sulla protezione dei dati Il regolamento (UE) 2016/679 e la direttiva di esecuzione (UE) 2016/680 del 30 giugno 2017 (Gazzetta ufficiale I pagina 2097) non sono conformi all'articolo 10 capoverso 1 della legge fondamentale o all'articolo 5 capoverso 1 frase 2 della legge fondamentale compatibile.

2. § 19 paragrafo 1, § 24 paragrafo 1 frase 1, paragrafo 2 frase 1, paragrafo 3 del Federal Intelligence Service Act non sono compatibili con l'articolo 10 paragrafo 1 della Legge fondamentale e con l'articolo 5 paragrafo 1 frase 2 della Legge fondamentale nella misura in cui sono utilizzati per elaborare autorizzare i dati personali raccolti in relazione alle informazioni strategiche sulle telecomunicazioni ai sensi delle sezioni 6, 7, 13-15 del Federal Intelligence Service Act.

3. Fino a un nuovo regolamento, ma non oltre il 31 dicembre 2021, continuano ad applicarsi i regolamenti dichiarati incompatibili con la Legge fondamentale.

4. La Repubblica federale di Germania deve rimborsare ai denuncianti le spese necessarie per la procedura di reclamo costituzionale.

Sommario

Motivi :

UN.

1

La denuncia costituzionale è diretta contro le autorizzazioni legali del Servizio di intelligence federale per la cosiddetta ricognizione delle telecomunicazioni estere-straniere, per la trasmissione delle conoscenze acquisite in tal modo a organismi nazionali ed esteri e per la cooperazione con i servizi di intelligence stranieri resi possibili in questo contesto. I regolamenti controversi, nella parte in cui riguardano l'educazione e la cooperazione in materia di telecomunicazioni, sono stati integrati nella legge sull'istruzione delle telecomunicazioni straniera e straniera dal Servizio di intelligence federale del 23 dicembre 2016 (Gazzetta federale I p. 3346) che è entrata in vigore il 31 dicembre 2016 (Gazzetta federale I p. 3346) Federal Intelligence Service (Legge BND - BNDG) del 20 dicembre 1990 (BGBl I S. 2954, 2979), modificato da ultimo dall'art.4 della legge sull'adeguamento della legge sulla protezione dei dati al regolamento (UE) 2016/679 e sull'attuazione della direttiva (UE) 2016/680 del 30 giugno 2017 (BGBl I p. 2097). In risposta ai risultati e alle discussioni del 1 ° comitato investigativo del 18 ° Bundestag tedesco (Comitato investigativo dell'NSA, cfr. Rapporto finale BTDrucks 18/12850), la modifica è servita a chiarire la situazione giuridica in merito a una prassi precedentemente esistente del Servizio federale di intelligence. Al contrario, i regolamenti controversi sulla trasmissione sono più vecchi e non sono

stati modificati nella loro formulazione dall'emendamento; tuttavia, ora si estendono anche alla trasmissione di conoscenze basate sui poteri di chiarimento di nuova concezione.In risposta ai risultati e alle discussioni del 1 ° comitato investigativo del 18 ° Bundestag tedesco (Comitato investigativo dell'NSA, cfr. Rapporto finale BTDrucks 18/12850), la modifica è servita a chiarire la situazione giuridica in merito a una prassi precedentemente esistente del Servizio federale di intelligence. Al contrario, i regolamenti controversi sulla trasmissione sono più vecchi e non sono stati modificati nella loro formulazione dall'emendamento; tuttavia, ora si estendono anche alla trasmissione di conoscenze basate sui poteri di chiarimento di nuova concezione.In risposta ai risultati e alle discussioni del 1 ° comitato investigativo del 18 ° Bundestag tedesco (Comitato investigativo dell'NSA, cfr. Rapporto finale BTDrucks 18/12850), la modifica è servita a chiarire la situazione giuridica in merito a una prassi precedentemente esistente del Servizio federale di intelligence. Al contrario, i regolamenti controversi sulla trasmissione sono più vecchi e non sono stati modificati nella loro formulazione dall'emendamento; tuttavia, ora si estendono anche alla trasmissione di conoscenze basate sui poteri di chiarimento di nuova concezione.Rapporto finale BTDrucks 18/12850) che chiarisce la situazione giuridica in merito a una pratica precedentemente esistente del Servizio di intelligence federale. Al contrario, i regolamenti controversi sulla trasmissione sono più vecchi e non sono stati modificati nella loro formulazione dall'emendamento; tuttavia, ora si estendono anche alla trasmissione di conoscenze basate sui poteri di chiarimento di nuova concezione.Rapporto finale BTDrucks 18/12850) che chiarisce la situazione giuridica in merito a una pratica precedentemente esistente del Servizio di intelligence federale. Al contrario, i regolamenti controversi sulla trasmissione sono più vecchi e non sono stati modificati nella loro formulazione dall'emendamento; tuttavia, ora si estendono anche alla trasmissione di conoscenze basate sui poteri di chiarimento di nuova concezione.

IO.

2 °

1. Le disposizioni contestate direttamente o indirettamente della legge BND e le disposizioni della legge federale sulla cooperazione tra la Federazione e i Länder in materia di protezione della costituzione e dell'Ufficio federale per la protezione della costituzione (Bundesverfassungsschutzgesetz - BVerfSchG) del 20 dicembre 1990 (BGBl I p. 2954, 2970) nella versione controversa dell'articolo 1 della legge sull'applicazione delle telecomunicazioni estere-straniere del Servizio di intelligence federale del 23 dicembre 2016 (BGBl I p. 3346) sono i seguenti:

§ 6 BNDG - Requisiti per la raccolta e l'elaborazione dei dati

(1) Per l'adempimento dei suoi compiti, il Servizio federale di intelligence può utilizzare la tecnologia per raccogliere ed elaborare informazioni, compresi dati personali da reti di telecomunicazioni, su quali stranieri all'estero (reti di telecomunicazioni) (reti di telecomunicazioni all'estero), se tali dati sono richiesti sono a

1. riconoscere tempestivamente i pericoli per la sicurezza interna o esterna della Repubblica federale di Germania ed essere in grado di contrastarli,

2. preservare la capacità di azione della Repubblica federale di Germania, o

3. acquisire ulteriori approfondimenti sull'importanza della politica estera e di sicurezza in merito a processi di tipo e ambito di applicazione della Cancelleria federale d'intesa con l'Ufficio federale degli affari esteri, il Ministero federale dell'interno, il Ministero federale della difesa, il Ministero

federale dell'economia e dell'energia e Ministero federale per la cooperazione e lo sviluppo economico.

I dati possono essere raccolti solo da quelle reti di telecomunicazione che la Cancelleria federale ha precedentemente determinato per ordine.

(2) Il servizio di intelligence federale può raccogliere dati di contenuto solo nell'ambito dell'educazione alle telecomunicazioni estere-estere utilizzando i termini di ricerca. Questi devono essere intesi e adatti al chiarimento dei fatti secondo il paragrafo 1 frase 1 e il loro uso deve essere conforme agli interessi di politica estera e di sicurezza della Repubblica Federale Tedesca.

(3) I termini di ricerca che conducono alla registrazione mirata delle istituzioni dell'Unione europea, degli enti pubblici dei suoi Stati membri o dei cittadini dell'Unione possono essere utilizzati solo se necessario,

1. riconoscere e contrastare i rischi ai sensi dell'articolo 5 capoverso 1 frase 3 della Legge sull'Articolo 10 o

2. ottenere informazioni ai sensi del paragrafo 1, frase 1, numeri da 1 a 3, nella misura in cui devono essere raccolti solo dati su eventi in paesi terzi che sono di particolare rilevanza per la sicurezza della Repubblica federale di Germania.

I termini di ricerca che portano alla registrazione mirata dei cittadini dell'Unione possono essere utilizzati anche se ciò è necessario per identificare e riscontrare reati ai sensi dell'articolo 3, paragrafo 1, della legge di cui all'articolo 10.

(4) La raccolta di dati dal traffico delle telecomunicazioni da parte di cittadini tedeschi, di persone giuridiche nazionali o di persone che si trovano nel territorio federale non è consentita.

(5) Non è consentito il chiarimento delle telecomunicazioni estere al fine di ottenere vantaggi competitivi (spionaggio industriale).

(6) I dati sul traffico sono conservati per un massimo di sei mesi. Le sezioni 19 e 20 rimangono inalterate.

(7) L'attuazione tecnica e organizzativa delle misure in conformità con il paragrafo 1 e le responsabilità di controllo nell'ambito del servizio di intelligence federale devono essere specificate in un regolamento di servizio che regola anche i dettagli della procedura di ordinazione. Il regolamento ufficiale richiede l'approvazione della Cancelleria federale. La Cancelleria federale informa l'organismo di controllo parlamentare.

Sezione 7 BNDG - Elaborazione e utilizzo dei dati raccolti dall'estero

(1) Sezione 6 sottosezione 1 frase 1 sottosezioni da 3 a 6 si applicano di conseguenza al trattamento e all'utilizzo dei dati raccolti dal Servizio federale di intelligence dall'estero mediante l'educazione alle telecomunicazioni.

(2) Il servizio di intelligence federale può provvedere alla registrazione delle istituzioni dell'Unione europea, degli enti pubblici nei suoi Stati membri o dei cittadini dell'Unione da parte di organismi pubblici stranieri provenienti dall'estero alle condizioni di cui al paragrafo 6, paragrafo 3.

§ 8 BNDG - Obblighi dei fornitori di servizi di telecomunicazione

(1) Chiunque fornisca servizi di telecomunicazione su base commerciale o partecipi alla fornitura di tali servizi deve, su richiesta, fornire al Servizio di intelligence federale informazioni sulle circostanze più ravvicinate delle telecomunicazioni effettuate dopo l'entrata in vigore dell'accordo e deve consegnare i programmi che gli sono affidati per la trasmissione attraverso la rotta delle telecomunicazioni e per consentire il monitoraggio e la registrazione delle telecomunicazioni. Le sezioni 3 e 4 rimangono inalterate. Se e in quale misura la società di telecomunicazioni obbligata debba prendere precauzioni per l'attuazione tecnica e organizzativa delle misure di sorveglianza è determinata in conformità alla Sezione 110 della legge sulle telecomunicazioni e all'ordinanza emessa a tale scopo.

(2) Prima di adottare una misura prevista, la società obbligata a norma del paragrafo 1 deve immediatamente disporre delle persone incaricate dell'attuazione della misura,

1. seleziona

2. sottoporsi a un semplice controllo di sicurezza e

3. istruire sul divieto di notifica ai sensi del § 17 e sulla punibilità di una violazione ai sensi del § 34; l'istruzione deve essere registrata.

Solo le persone che sono state controllate e istruite conformemente alla frase 1 possono essere incaricate dell'attuazione di una misura. Dopo l'approvazione della Cancelleria federale, il capo del Servizio di intelligence federale o un rappresentante può richiedere per iscritto alle società obbligate ai sensi del paragrafo 1 di eseguire la misura prima che il controllo di sicurezza sia stato completato. Le società obbligate ai sensi del paragrafo 1 devono garantire che le misure di protezione segreta ai sensi del regolamento amministrativo generale del Ministero federale dell'interno per la protezione materiale e organizzativa delle informazioni classificate del 31 marzo 2006 (GMBl p. 803), più recentemente dal regolamento amministrativo generale del 26 aprile 2010 (GMBl p. 846) è stato modificato,nella versione attualmente applicabile.

(3) Il controllo di sicurezza secondo il paragrafo 2 frase 1 numero 2 deve essere effettuato in conformità con il Security Check Act. Il Ministero federale dell'interno è responsabile. Se una persona deve essere incaricata dell'attuazione di una misura, per la quale un controllo di sicurezza equivalente o di livello superiore secondo la legge federale o statale è già stato effettuato negli ultimi cinque anni, dovrebbe essere evitato un nuovo controllo di sicurezza.

Sezione 9 BNDG - Ordine; Riunione

(1) L'ordinanza ai sensi dell'articolo 6, paragrafo 1, viene effettuata per iscritto su richiesta del capo del Servizio di intelligence federale o di un rappresentante. La domanda e l'ordine devono indicare:

1. il motivo e la durata della misura,

2. anche la rete di telecomunicazioni interessata

3. la società obbligata ai sensi del § 8.

(2) L'ordine del capo dell'autorità o di un rappresentante richiede che vengano determinati i termini di ricerca

1. ai sensi del § 6 capoverso 3 frase 1 numero 1, nella misura in cui si riferiscono alle istituzioni dell'Unione europea o agli enti pubblici dei loro Stati membri nonché

2. secondo § 6 paragrafo 3 frase 1 numero 2.

La Cancelleria federale deve essere informata degli ordini ai sensi della frase 1.

(3) Gli ordini di cui al paragrafo 2 e § 6 paragrafo 1 sono limitati a un massimo di nove mesi. Sono consentite estensioni fino a nove mesi, a condizione che i requisiti dell'ordine continuino.

(4) La Cancelleria federale informa l'organismo indipendente degli ordini effettuati a norma dell'articolo 6, paragrafo 1, prima che siano eseguiti. Il comitato indipendente verifica l'ammissibilità e la necessità dell'ordine. L'ordine può essere eseguito senza informare preventivamente il gruppo indipendente se l'obiettivo della misura sarebbe altrimenti frustrato o reso notevolmente più difficile. In tal caso, le informazioni del comitato indipendente devono essere raccolte immediatamente. Gli ordini che il panel indipendente dichiara inammissibili o non necessari devono essere immediatamente revocati.

(5) La Cancelleria federale informa l'organismo indipendente degli ordini effettuati dal Servizio di intelligence federale conformemente al paragrafo 2, nella misura in cui si riferiscono ad istituzioni dell'Unione europea o ad enti pubblici nei suoi Stati membri. Gli ordini che il panel indipendente dichiara inammissibili o non necessari devono essere immediatamente revocati. Il Comitato Indipendente è inoltre autorizzato a verificare casualmente la conformità ai requisiti della Sezione 6 (3) in qualsiasi momento. I diritti di controllo dell'organismo di controllo parlamentare rimangono inalterati.

§ 10 BNDG - marcatura ed eliminazione

(1) I dati raccolti in base al § 6 devono essere contrassegnati.

(2) Se un ordine secondo § 9 paragrafo 5 frase 2 viene cancellato, i dati già raccolti a causa di questo ordine devono essere immediatamente cancellati.

(3) Se i dati vengono raccolti in contrasto con § 6 paragrafo 3 o § 9 paragrafo 2, devono essere immediatamente cancellati. Il gruppo indipendente deve essere informato di ciò. Se successivamente viene riconosciuto che un termine di ricerca deve essere assegnato a un'istituzione dell'Unione Europea, a un ente pubblico di uno stato membro o un cittadino dell'Unione, anche il traffico di telecomunicazioni raccolto utilizzando questo termine di ricerca deve essere immediatamente cancellato, a meno che una voce mirata secondo § 6 Il paragrafo 3 sarebbe stato ammissibile.

(4) Se i dati vengono raccolti in violazione dell'articolo 6, paragrafo 4, devono essere immediatamente cancellati. Se i dati non vengono cancellati immediatamente, la Commissione G10 deve essere informata nella riunione successiva e l'interessato deve essere informato della raccolta dei dati non appena

1. Si può escludere che lo scopo della misura sia in pericolo e

2. non è prevedibile alcuno svantaggio per il bene del governo federale o di un paese.

Se la notifica non viene effettuata entro dodici mesi dalla raccolta dei dati, l'ulteriore differimento richiede l'approvazione della Commissione G10. La commissione G10 determina l'ulteriore durata del differimento. Cinque anni dopo che i dati sono stati raccolti, la Commissione G10 può finalmente rinunciare alla notifica se le condizioni per la notifica non saranno quasi certamente soddisfatte in futuro. Finché i dati personali possono essere importanti per una notifica o per un controllo giurisdizionale della raccolta dei dati, la cancellazione sarà rinviata e i dati personali saranno bloccati; possono essere utilizzati solo per questi scopi.

(5) Se i dati vengono raccolti in violazione dell'articolo 6, paragrafo 5, devono essere immediatamente cancellati.

(6) Le soppressioni conformemente ai paragrafi da 2 a 5 devono essere registrate. I dati di registro possono essere utilizzati solo per eseguire controlli di protezione dei dati. I dati del registro devono essere conservati fino alla fine del secondo anno solare successivo alla registrazione e quindi eliminati immediatamente.

Sezione 11 BNDG - protezione dell'area centrale

Se ci sono indicazioni concrete per l'assunto che una misura secondo la sola Sezione 6 fornirebbe approfondimenti dall'area centrale del progetto di vita privata, la misura è inammissibile. Nella misura in cui le conoscenze provenienti dall'area centrale della progettazione della vita privata sono state ottenute attraverso una misura ai sensi del § 6, queste non possono essere utilizzate. Le registrazioni di tali conoscenze devono essere immediatamente cancellate. Sia la loro acquisizione che la loro cancellazione devono essere registrate.

Sezione 13 BNDG - Cooperazione nel contesto dell'educazione alle telecomunicazioni estero-straniera

(1) Nella misura in cui il Servizio di intelligence federale coopera con enti pubblici stranieri che svolgono compiti di intelligence (enti pubblici stranieri) nell'ambito dell'educazione alle telecomunicazioni estere (Sezione 6), anche le informazioni, compresi i dati personali, possono essere raccolte in conformità con la Sezione 14 e scambiate in conformità con la Sezione 15 volere.

(2) È consentita una cooperazione ai sensi del paragrafo 1 con un ente pubblico straniero se

1. serve gli obiettivi della sezione 6 sottosezione 1 frase 1 numeri da 1 a 3 e

2. l'adempimento di compiti da parte del Servizio di intelligence federale sarebbe significativamente più difficile o impossibile senza tale cooperazione.

(3) I dettagli della cooperazione devono essere indicati per iscritto in una lettera di intenti tra il Servizio di intelligence federale e l'ente pubblico straniero prima che inizi. In particolare, la dichiarazione di intenti deve includere:

1. obiettivi di cooperazione,

2. Contenuto della cooperazione,

3. durata della cooperazione,

4. un accordo che i dati raccolti nel contesto della cooperazione possono essere utilizzati solo per lo scopo per il quale sono stati raccolti e che l'uso deve essere compatibile con i principi fondamentali dello stato di diritto,

5. un accordo in base al quale l'autorità pubblica estera si impegna a fornire informazioni sull'uso dei dati fatte su richiesta del Servizio di intelligence federale, e

6. una garanzia da parte dell'ente pubblico straniero di soddisfare una richiesta di annullamento da parte del Servizio di intelligence federale.

(4) Gli obiettivi e i contenuti della cooperazione devono mirare a ottenere informazioni

1. identificare e contrastare i pericoli posti dal terrorismo internazionale,

2. identificare e contrastare i pericoli posti dalla proliferazione illegale di armi di distruzione di massa e di guerra,

3. sostenere la Bundeswehr e proteggere le forze armate dei paesi coinvolti nella cooperazione,

4. sviluppi connessi alla crisi all'estero,

5. sulla situazione di rischio e sicurezza dei cittadini tedeschi e dei cittadini dei paesi che partecipano alla cooperazione all'estero,

6. eventi politici, economici o militari all'estero aventi rilevanza per la politica estera e di sicurezza o

7. in casi comparabili.

(5) La dichiarazione di intenti richiede l'approvazione della Cancelleria federale qualora avvenga la cooperazione con enti pubblici stranieri degli Stati membri dell'Unione Europea, dello Spazio economico europeo o del Trattato del Nord Atlantico; altrimenti richiede l'approvazione del capo della Cancelleria federale. L'organismo di controllo parlamentare deve essere informato della dichiarazione di intenti.

Sezione 14 BNDG - Raccolta di informazioni inclusi dati personali nel contesto di una cooperazione

(1) Il servizio di intelligence federale può raccogliere informazioni, compresi dati personali, nell'ambito di una cooperazione ai sensi dell'articolo 13,

1. per raggiungere gli obiettivi di cooperazione concordati,

2. Se vengono utilizzati solo quei termini di ricerca quando si raccolgono dati di contenuto idonei al raggiungimento degli obiettivi di cooperazione concordati.

La raccolta di informazioni, inclusi dati personali e l'uso di termini di ricerca, deve essere conforme agli interessi di politica estera e di sicurezza della Repubblica Federale Tedesca.

(2) Inoltre, § 6 paragrafo 1 frase 2, paragrafi da 3 a 7 e §§ da 8 a 12 si applicano di conseguenza.

(3) Le telecomunicazioni all'estero-all'estero possono essere effettuate dal servizio di intelligence federale stesso nell'ambito di una cooperazione ai sensi dell'articolo 13.

§ 15 BNDG - Trasmissione automatizzata di dati; Conservazione; esame

(1) Le informazioni raccolte nell'ambito della cooperazione, compresi i dati personali, possono essere automaticamente trasmesse all'ente pubblico straniero se

1. riconosciuto in anticipo da un test automatizzato

a) Dati secondo § 10 capoverso 3 e 4 o

b) i dati la cui trasmissione sarebbe in conflitto con gli interessi nazionali della Repubblica federale di Germania,

sono stati eliminati e

2. La trasmissione immediata è necessaria per raggiungere gli obiettivi della cooperazione.

(2) La trasmissione dei dati deve essere registrata. I dati di registro possono essere utilizzati solo per eseguire controlli di protezione dei dati. I dati del registro devono essere conservati fino alla fine del secondo anno solare successivo alla registrazione e quindi eliminati immediatamente.

(3) Il rispetto dei requisiti di cui al paragrafo 1 e § 11 è verificato su base casuale. L'esame viene svolto sotto la supervisione di un membro del Servizio di intelligence federale che ha le qualifiche per agire come giudice. Se successivamente viene riconosciuto che i dati sono stati raccolti in violazione di queste specifiche e trasmessi a un ente pubblico straniero, si richiede all'ente pubblico straniero di cancellare i dati. Il Servizio di intelligence federale informa la Cancelleria federale a intervalli non superiori a sei mesi sullo svolgimento dell'esame conformemente alla frase 1. I dettagli devono essere regolati in un regolamento di servizio che richiede l'approvazione della Cancelleria federale. La Cancelleria federale informa l'organismo di controllo parlamentare.Il comitato indipendente può verificare casualmente la conformità ai requisiti di cui al paragrafo 1 e § 11 in qualsiasi momento.

(4) I dati raccolti nel contesto della cooperazione sulla base dei termini di ricerca specificati dall'autorità pubblica estera saranno conservati dal Servizio di intelligence federale per un periodo di due settimane. Le sezioni 19 e 20 rimangono inalterate.

Sezione 16 BNDG - Organismo indipendente

(1) Il gruppo indipendente è composto da

1. un presidente,

2. due valutatori e

3. tre membri supplenti.

I membri del consiglio di amministrazione indipendente e i membri supplenti del consiglio di amministrazione indipendente sono indipendenti nel loro ufficio e non sono soggetti alle istruzioni. Il presidente e un perito sono giudici presso la Corte federale di giustizia, l'altro perito è un

procuratore federale presso la Corte federale di giustizia o un procuratore federale presso la Corte federale di giustizia. Due membri supplenti sono giudici donne presso la Corte federale di giustizia, un membro supplente è un procuratore federale presso la Corte federale di giustizia o un procuratore federale presso la Corte federale di giustizia.

(2) Il Gabinetto federale nomina per un periodo di sei anni

1. su proposta del presidente della Corte federale di giustizia, i membri dell'organo indipendente che sono giudici presso la Corte federale di giustizia o giudici presso la Corte federale di giustizia, compresi i loro deputati e

2. su proposta del Procuratore generale federale, membro del Comitato indipendente, che è procuratore federale presso la Corte federale di giustizia o procuratore federale presso la Corte federale di giustizia, compreso il suo supplente.

(3) Il comitato indipendente deve essere dotato del personale e delle attrezzature materiali necessarie per lo svolgimento dei suoi compiti. L'ufficio è istituito presso la Corte di giustizia federale.

(4) Il gruppo indipendente si riunisce almeno ogni tre mesi. Ci sono regole di procedura. Il gruppo indipendente decide con la maggioranza dei voti. Se uno o più membri vengono impediti, il rispettivo vice prende parte alla riunione.

(5) Le deliberazioni del gruppo indipendente sono segrete. I membri, nonché i membri supplenti del consiglio di amministrazione indipendente e i dipendenti dell'ufficio sono tenuti a mantenere riservate le questioni che sono diventate loro note in o in occasione del loro lavoro nel consiglio di amministrazione. Ciò vale anche per il periodo successivo alla sua uscita dal consiglio di amministrazione indipendente. I dipendenti dell'ufficio devono sottoporsi a un controllo di sicurezza esteso con indagini di sicurezza (Sezione 7, paragrafo 1, numero 3 del Security Check Act).

6. Il panel indipendente informa il panel di controllo parlamentare delle sue attività a intervalli non superiori a sei mesi.

Sezione 19 BNDG - conservazione, modifica e utilizzo dei dati personali

(1) Il servizio di intelligence federale può salvare, modificare e utilizzare i dati personali in conformità con la sezione 10 della legge sulla protezione della costituzione federale, nella misura in cui è necessario per adempiere ai suoi compiti.

(2) La conservazione, la modifica e l'uso di dati personali su minori sono consentiti solo alle condizioni della Sezione 11 della Legge sulla protezione costituzionale federale e se, nelle circostanze del singolo caso, non si può escludere che il minore possa mettere in pericolo la vita o l'arto dei cittadini tedeschi all'estero o per istituzioni tedesche all'estero.

Sezione 20 BNDG - correzione, cancellazione e blocco dei dati personali

(1) Il servizio di intelligence federale deve correggere, eliminare e bloccare i dati personali archiviati in file conformemente alla sezione 12 della legge sulla protezione costituzionale federale, a condizione che il periodo di esame in conformità alla sezione 12 (3) frase 1 della legge sulla protezione costituzionale federale sia di dieci anni.

(2) Il servizio di intelligence federale deve correggere e bloccare i dati personali in file secondo § 13 capoversi 1 e 2 della legge sulla protezione della costituzione federale. Per l'uso di file elettronici, si applica l'articolo 13 capoverso 4 della legge federale sulla protezione costituzionale, con la condizione che la necessità dei file elettronici per l'adempimento dei compiti deve essere verificata al più tardi dopo dieci anni.

Sezione 24 BNDG - Trasmissione di informazioni da parte del Servizio di intelligence federale

(1) Il servizio di intelligence federale può trasmettere informazioni, compresi dati personali, a enti pubblici nazionali se ciò è necessario per lo svolgimento dei suoi compiti o se il destinatario ha bisogno dei dati per scopi significativi di pubblica sicurezza. Può solo trasmettere le informazioni, compresi i dati personali, che sono state raccolte utilizzando i mezzi di cui alla Sezione 5 agli organismi specificati nella Sezione 19, comma 1, frase 1 della Legge sulla protezione costituzionale federale alle condizioni ivi specificate o ai sensi della Sezione 3. Salvo quanto diversamente stabilito dalla legge, il destinatario può utilizzare i dati trasmessi solo per lo scopo per il quale sono stati trasmessi.

(2) Sezione 19 sottosezioni da 2 a 5 della legge sulla protezione costituzionale federale si applicano, mutatis mutandis, alla trasmissione di informazioni, compresi i dati personali; la trasmissione ai sensi del paragrafo 4 del presente regolamento è consentita solo se è necessaria per tutelare gli interessi di politica estera e di sicurezza della Repubblica federale di Germania e se la Cancelleria federale ha dato il proprio consenso. Per i dati personali trasmessi dall'Ufficio federale per la protezione della Costituzione ai sensi della Sezione 18 (1a) frase 1 della Legge sulla protezione costituzionale federale, si applicano di conseguenza le sezioni da 2 a 4 della Sezione 18 (1a) della Legge federale sulla protezione costituzionale.

(3) Il servizio di intelligence federale trasmette informazioni, compresi i dati personali, all'ufficio del procuratore, alla polizia e al servizio di protezione militare conformemente alla sezione 20 della legge sulla protezione della costituzione federale.

3 °

Le disposizioni di riferimento del Federal Constitution Protection Act sono le seguenti:

§ 10 BVerfSchG - conservazione, modifica e utilizzo dei dati personali

(1) L'Ufficio federale per la protezione della Costituzione può salvare, modificare e utilizzare i dati personali nei file per adempiere ai suoi compiti se

1. vi sono indicazioni effettive di sforzi o attività ai sensi dell'articolo 3, paragrafo 1,

2. ciò è necessario per la ricerca e la valutazione di sforzi o attività ai sensi del § 3 comma 1 o

3. l'Ufficio federale per la protezione della Costituzione agisce conformemente alla sezione 3 (2).

(2) I documenti a supporto dei dati archiviati in conformità al paragrafo 1 possono anche essere salvati se contengono altri dati personali di terzi. Non è consentita una query di dati di terze parti.

(3) L'Ufficio federale per la protezione della Costituzione limita il periodo di conservazione nella misura necessaria allo svolgimento dei suoi compiti.

§ 12 BVerfSchG - correzione, cancellazione e blocco dei dati personali nei file

(1) L'Ufficio federale per la protezione della Costituzione deve correggere i dati personali archiviati nei file se non sono corretti.

(2) L'Ufficio federale per la protezione della Costituzione cancella i dati personali archiviati in file se la loro conservazione era inammissibile o se la loro conoscenza non è più necessaria per l'esecuzione dell'attività. La cancellazione non avverrà se c'è motivo di ritenere che ciò pregiudicherebbe gli interessi della persona interessata che vale la pena proteggere. In questo caso, i dati devono essere bloccati. Possono essere trasmessi solo con il consenso dell'interessato.

(3) L'Ufficio federale per la protezione della Costituzione verifica se i singoli dati debbano essere corretti o cancellati al più tardi dopo cinque anni nell'elaborazione dei casi e dopo scadenze specifiche. I dati personali memorizzati sugli sforzi di cui al § 3 capoverso 1 numeri 1, 3 e 4 devono essere cancellati al più tardi dieci anni dopo il momento dell'ultima informazione salvata pertinente, a meno che la direzione del dipartimento responsabile o il loro rappresentante non prendano una decisione diversa in casi eccezionali.

(4) I dati personali archiviati esclusivamente ai fini del controllo della protezione dei dati, del backup dei dati o per garantire il corretto funzionamento di un sistema di elaborazione dei dati possono essere utilizzati solo per tali scopi.

§ 18 BVerfSchG - Trasmissione di informazioni alle autorità di protezione costituzionale

(1) […]

(1 bis) L'Ufficio federale della migrazione e dei rifugiati si trasmette dall'Ufficio federale per la protezione della Costituzione, le autorità di immigrazione di un paese trasmettono informazioni che sono state loro conosciute dall'agenzia di protezione costituzionale del paese, compresi i dati personali sugli sforzi o attività secondo la Sezione 3 (1), se effettivi Vi sono indicazioni che la trasmissione è necessaria per l'adempimento dei compiti dell'autorità di protezione costituzionale. La trasmissione di questi dati personali a enti pubblici stranieri nonché a organismi sovranazionali e intergovernativi in conformità con la Sezione 19 (3) non ha luogo anche se vi sono interessi prevalenti degni di protezione da parte di terzi. L'Ufficio federale della migrazione e dei rifugiati deve essere coinvolto prima di un trasferimento conformemente alla sezione 19 (3).La sezione 8b (3) si applica di conseguenza a questi trasferimenti da parte dell'Ufficio federale per la protezione della Costituzione. [...]

(1b) - (6) […]

Sezione 19 BVerfSchG - Trasmissione di dati personali da parte dell'Ufficio federale per la protezione della Costituzione

(1) L'Ufficio federale per la protezione della Costituzione può dati personali, che sono stati raccolti con i mezzi di cui al § 8 paragrafo 2, alla Procura della Repubblica, alle autorità finanziarie ai sensi del § 386 capoverso 1 del codice fiscale, alla polizia, ai dipartimenti di indagine fiscale delle autorità fiscali statali, trasmettere le autorità del servizio investigativo doganale e altri servizi doganali, nella misura in cui questi svolgono compiti ai sensi della legge federale sulla polizia, nella misura in cui ciò è necessario per

1. adempimento dei propri compiti di acquisizione delle informazioni (§ 8 capoverso 1 frasi 2 e 3),

2. Evitare un rischio in singoli casi per l'esistenza o la sicurezza del governo federale o di un paese o per la vita, l'arto, la salute o la libertà di una persona o per cose di notevole valore, la cui conservazione è nell'interesse pubblico,

3. Prevenzione o altra prevenzione di reati significativi o

4. perseguimento di reati di primaria importanza;

La sezione 20 rimane inalterata. [...]

(2) L'Ufficio federale per la protezione della Costituzione può trasmettere dati personali alle forze armate di stanza, nella misura in cui la Repubblica federale di Germania lo fa nell'ambito dell'articolo 3 dell'accordo aggiuntivo all'accordo tra le parti del trattato del Nord Atlantico sullo status giuridico delle sue truppe in relazione alle truppe straniere di stanza nella Repubblica federale di Germania del 3 agosto 1959 (Gazzetta federale 1961 II p. 1183, 1218).

(3) L'Ufficio federale per la protezione della Costituzione può trasmettere dati personali a organismi pubblici stranieri nonché a organismi sovranazionali e intergovernativi se la trasmissione è necessaria per adempiere ai suoi compiti o per salvaguardare gli interessi significativi di sicurezza del destinatario. La trasmissione non avverrà se interessi stranieri della Repubblica Federale Tedesca o interessi predominanti degni di protezione entrano in conflitto con l'interessato. La trasmissione deve essere registrata. Il destinatario deve essere informato che i dati trasmessi possono essere utilizzati esclusivamente per lo scopo per il quale sono stati trasmessi e l'Ufficio federale per la protezione della Costituzione si riserva il diritto di richiedere informazioni sull'uso dei dati.

(4) I dati personali possono essere trasferiti in altri luoghi solo per proteggere l'ordine di base democratico libero, l'esistenza o la sicurezza del governo federale o di un paese o per garantire la sicurezza di strutture vitali o legate alla difesa ai sensi del § 1 paragrafo 4 del È richiesta la legge sul nulla osta di sicurezza. Le trasmissioni ai sensi della frase 1 richiedono il consenso preventivo del Ministero federale dell'interno. L'Ufficio federale per la protezione della Costituzione fornisce la prova dello scopo, della causa, del sito di individuazione dei file e dei destinatari dei trasferimenti conformemente alla frase 1. Le prove devono essere conservate separatamente, assicurate contro l'accesso non autorizzato e alla fine dell'anno civile che segue l'anno in cui è stata creata distruggere.Il destinatario può utilizzare i dati trasmessi solo per lo scopo per il quale sono stati trasmessi. Il destinatario deve essere informato della limitazione dell'uso e che l'Ufficio federale per la protezione della Costituzione si riserva il diritto di richiedere informazioni sull'uso dei dati. L'Ufficio federale per la protezione della Costituzione notifica all'interessato il trasferimento dei dati personali non appena non sussiste più alcun pericolo per l'adempimento delle sue funzioni dalla notifica.L'Ufficio federale per la protezione della Costituzione notifica all'interessato il trasferimento dei dati personali non appena non sussiste più alcun pericolo per l'adempimento delle sue funzioni dalla notifica.L'Ufficio federale per la protezione della Costituzione notifica all'interessato il trasferimento dei dati personali non appena non sussiste più alcun pericolo per l'adempimento delle sue funzioni dalla notifica.

(5) Il paragrafo 4 non si applica se i dati personali sono trasmessi ai fini della raccolta dei dati conformemente alla sezione 8, paragrafo 1, frase 2, agli organismi da cui i dati vengono raccolti o che cooperano con essi. In deroga a ciò, si applicano le frasi 5 e 6 del paragrafo 4 nei casi in cui i dati non vengono raccolti utilizzando i mezzi specificati nel § 8 paragrafo 2.

Sezione 20 BVerfSchG - Trasmissione di informazioni da parte dell'Ufficio federale per la protezione della Costituzione alle autorità di contrasto e di sicurezza in materia di protezione statale e costituzionale

(1) L'Ufficio federale per la protezione della Costituzione trasmette alle Procure della Repubblica e, fatta salva l'autorità del pubblico ministero, la polizia, di propria iniziativa, le informazioni che le sono divenute note, compresi i dati personali, se vi sono indicazioni concrete che la trasmissione è necessaria per prevenire o perseguire i reati di sicurezza dello stato è. I reati di cui alla frase 1 sono i reati menzionati nelle sezioni 74a e 120 della legge costituzionale della Corte nonché altri reati che, in base al loro scopo, al motivo del colpevole o al loro collegamento con un'organizzazione, forniscono indicazioni concrete di violazione delle disposizioni dell'articolo 73 no Sono indirizzate 10 lettere b o c della Legge fondamentale.L'Ufficio federale per la protezione della Costituzione trasmette al Servizio di intelligence federale, di propria iniziativa, le informazioni che gli sono diventate note, compresi i dati personali, se vi sono indicazioni concrete che la trasmissione è necessaria per l'adempimento dei compiti legali del destinatario.

(2) […] [Richieste di presentazione da parte della polizia e del BND]

4 °

2. L'educazione alle telecomunicazioni estere-straniere mira esclusivamente alla sorveglianza del traffico di telecomunicazione degli stranieri situati all'estero. È integrato nel compito di intelligence generale del Servizio di intelligence federale, che, conformemente alla sezione 1, paragrafo 2, frase 1, BNDG, consiste nel raccogliere le informazioni necessarie per acquisire conoscenze su paesi stranieri che hanno un significato di politica estera e di sicurezza per la Repubblica federale di Germania e valutare.

5

Il servizio di intelligence federale utilizza varie fonti di informazione per svolgere la propria missione di informazione. Questi possono essere suddivisi in quattro pilastri, vale a dire la raccolta e la valutazione delle fonti generalmente disponibili, la valutazione del materiale dell'immagine - principalmente ottenuta da satelliti - la raccolta e la valutazione delle informazioni ottenute da fonti umane e la televisione effettuata dal dipartimento di educazione tecnica - Sorveglianza della comunicazione ("signal intelligence", SIGINT), alla quale appartiene la ricognizione strategica delle telecomunicazioni estere-estere. Secondo il governo federale, circa il 50 percento delle relazioni totali generate dal servizio di intelligence federale si basa sull'emergere del dipartimento di intelligence tecnica,Il 36 percento dei rapporti, e quindi una media di 260 al giorno, proviene dal chiarimento delle telecomunicazioni estere in questione.

6

I regolamenti contestati regolano la cosiddetta sorveglianza strategica delle telecomunicazioni. Ciò è caratterizzato dal fatto che si riferisce a percorsi o reti di trasmissione di telecomunicazione e mira a filtrare quelli della totalità dei dati di telecomunicazione trasmessi nelle reti che sono rilevanti per l'intelligence. Di conseguenza, ha inevitabilmente una vasta gamma e in genere non è collegato a occasioni o sospetti specifici. Invece, lavora in anticipo e mira principalmente a ottenere indizi, sospetti, conoscenze generali e rapporti sulla situazione su argomenti che sono interessati dal mandato del governo federale (vedi § 6 Paragrafo 1 Clausola 1 n. 3 BNDG, di solito abbreviato “APB”) ; più vicino al marg.9) si dimostrano significativi per la politica estera e di sicurezza della

Repubblica federale. Inoltre, i mezzi di sorveglianza strategica delle telecomunicazioni si aprono e mirano a educare individui specifici.

7

Oltre al potere di monitorare strategicamente le telecomunicazioni degli stranieri che sono all'estero, il Servizio di intelligence federale ha - oltre al potere di limitare singoli casi - il potere di monitorare strategicamente il traffico internazionale di telecomunicazioni, vale a dire le telecomunicazioni tra stranieri che sono all'estero da un lato e cittadini o tedeschi dall'altra parte. Questi poteri sono - e non sono in discussione qui - nell'articolo 10 del 26 giugno 2001 (BGBl I p. 1254, 2298), modificato da ultimo dall'articolo 12 della legge del 17 agosto 2017 (BGBl I p. 3202) legalmente diverso. Altre autorità, in particolare l'Ufficio federale per la protezione della Costituzione come servizio di intelligence nazionale, non dispongono di tali poteri.

8 °

3. I regolamenti impugnati stabiliscono norme specifiche sia per la raccolta di dati dall'interno della Germania sia per il suo trattamento (sezione 6 BNDG) e per l'ulteriore trattamento dei dati raccolti dall'estero (sezione 7 (1) BNDG). § 7 BNDG deliberatamente non regola una norma di autorizzazione espressa per la raccolta di dati personali dall'estero e non contiene la legge BND in nessun altro modo. Il legislatore presume che non sia necessaria una base di intervento e che la raccolta dei dati possa basarsi esclusivamente sullo standard di attività nella Sezione 1 (2) BNDG, poiché non esiste alcuna relazione vincolante con i diritti fondamentali della Legge fondamentale (cfr. BTDrucks 18/9041, p. 25).

9

La Cancelleria federale, in accordo con gli altri ministeri federali che operano nel campo della politica estera e di sicurezza (cfr. Sezione 6 (1) frase 1 n. 3 BNDG), determina il focus, la profondità e le priorità delle misure di sorveglianza sulla base dei regolamenti impugnati. Profilo dell'ordine riservato del governo federale specificato. Inoltre, secondo il governo federale, ci sono anche ordini individuali a breve termine della Cancelleria federale. La sezione 6 (1) frase 1 n. 1 e 2 BNDG consente inoltre al servizio di eseguire misure di sorveglianza indipendentemente dagli ordini del governo federale.

10 °

Tutte le informazioni e i dati provenienti dalle reti determinati dall'ordinamento della Cancelleria federale possono essere raccolti ("accordo di rete", vedere § 6 Paragrafo 1 Frase 2, § 9 Paragrafi 1, 3 e 4 BNDG). Un'eccezione si applica solo ai dati delle transazioni di telecomunicazione che coinvolgono tedeschi o residenti (Sezione 6 (4) BNDG); In pratica, il regolamento è inteso in modo tale che i suoi dati possano inizialmente essere registrati, ma poi, se possibile, deve essere filtrato senza valutare il contenuto. Ciò include i dati sul traffico e sui contenuti provenienti dai processi di telecomunicazione tra le persone, nonché - secondo il governo federale sulla gestione della normativa in pratica - altri dati trasportati nelle reti dalla comunicazione uomo a macchina o da macchina a macchina,come, ad esempio, i dati di localizzazione generati automaticamente per i telefoni cellulari accesi. I dati di contenuto delle telecomunicazioni possono essere raccolti solo sulla base dei termini di ricerca utilizzati per chiarire le questioni relative alle informazioni di legge sono idonei e necessari (Sezione 6 (2) BNDG). La raccolta mirata di telecomunicazioni da parte dei cittadini dell'Unione e gli enti pubblici dell'Unione Europea o dei suoi stati membri sono soggetti a sostanziali sostanziali (Sezione 6 (3) BNDG) e in alcuni casi anche diritto processuale (Sezione 9

(2) e (5) BNDG). La raccolta e l'elaborazione dei dati a fini di spionaggio industriale non sono consentite (Sezione 6 (5) BNDG). I dati sul traffico, che in pratica includono non solo i dati delle telecomunicazioni tra le persone, ma anche altri (meta) dati personali trasportati nelle reti, possono essere conservati per un periodo massimo di sei mesi (§ 6 cpv. 6 frase 1 BNDG) e sono soggetti a elaborazione e valutazione non specificate.In caso di un'esigenza specifica di intelligence, può essere giustificata anche una conservazione più lunga (Sezione 6 (6) frase 2 BNDG). Sezione 7 BNDG regola l'ulteriore trattamento dei dati di telecomunicazione raccolti dall'estero; egli stesso non regola l'autorità per raccoglierli, ma li presuppone.

11

Nella misura in cui ciò è tecnicamente necessario, i fornitori di servizi di telecomunicazione sono tenuti ad abilitare e partecipare alla raccolta di dati in conformità con la sezione 8 BNDG sul corrispondente accordo di diversione. La sezione 9 BNDG regola la procedura per l'organizzazione delle reti da registrare e la definizione di termini di ricerca in casi speciali per proteggere dalla registrazione mirata di determinati attori nell'Unione europea, compreso un certo controllo di tali requisiti da parte dell'organismo indipendente da istituire conformemente alla sezione 16 BNDG. Secondo la Sezione 10 Paragrafo 1 BNDG, i dati raccolti devono essere identificati e, in conformità con la Sezione 10 Paragrafi da 2 a 5 BNDG, sono soggetti a cancellazione in caso di raccolta inammissibile. In deroga a ciò, la Sezione 10 (4) frasi da 2 a 6 del BNDG impone requisiti procedurali speciali per il casoche non vi è alcuna cancellazione immediata della comunicazione con la partecipazione successivamente riconosciuta di tedeschi o residenti. Le disposizioni legali per proteggere l'area centrale della vita personale sono regolate nel § 11 BNDG.

12

4. Le sezioni da 13 a 15 del BNDG regolano la cooperazione del Servizio di intelligence federale con i servizi di intelligence esteri, compresa la trasmissione automatizzata di dati a enti pubblici stranieri. I regolamenti consentono - in larga misura con riferimento ai requisiti di raccolta dei dati appena spiegati (Sezione 14 (2) BNDG) - nella misura in cui la raccolta di dati per la sorveglianza strategica delle telecomunicazioni da parte del Servizio federale di intelligence anche a favore dei servizi di intelligence cooperanti (Sezione 14 BNDG). La base è una dichiarazione di intenti congiunta più dettagliata (§ 13 BNDG) e gli obiettivi di cooperazione ivi stabiliti. In particolare, è consentito il confronto dei dati di telecomunicazione registrati dal Servizio federale di intelligence con i termini di ricerca specificati dai servizi partner (Sezione 14 (1) frase 1 BNDG).Basandosi su questo, il regolamento autorizza quindi il Servizio di intelligence federale - in conformità con i requisiti sostanziali e procedurali speciali (Sezione 15, paragrafi 1 e 2 BNDG), che includono il filtraggio automatico delle comunicazioni nazionali e internazionali - per trasmettere automaticamente il traffico di dati selezionato utilizzando termini di ricerca denominati esternamente ai partner della cooperazione. Inoltre, è consentita la trasmissione automatizzata di dati sul traffico non selezionati (Sezione 15 (1) BNDG). La ricezione e l'elaborazione dei dati raccolti da servizi stranieri nell'ambito della cooperazione e trasmessi al Servizio di intelligence federale sono regolati dalle sezioni 14 f. BNDG non specificoche include il filtraggio automatico della comunicazione nazionale e internazionale - per la trasmissione automatizzata del traffico di dati selezionato utilizzando termini di ricerca denominati esternamente ai partner della cooperazione. Inoltre, è consentita la trasmissione automatizzata di dati sul traffico non selezionati (Sezione 15 (1) BNDG). La ricezione e l'elaborazione dei dati raccolti da servizi stranieri nell'ambito della cooperazione e trasmessi al Servizio di intelligence federale sono regolati dalle sezioni 14 f. BNDG non specificoche include il filtraggio automatico della comunicazione nazionale e internazionale - per la trasmissione automatizzata del traffico di dati selezionato utilizzando termini di ricerca denominati esternamente ai partner della cooperazione. Inoltre, è

consentita la trasmissione automatizzata di dati sul traffico non selezionati (Sezione 15 (1) BNDG). La ricezione e l'elaborazione dei dati raccolti da servizi stranieri nell'ambito della cooperazione e trasmessi al Servizio di intelligence federale sono regolati dalle sezioni 14 f. BNDG non specificoLa ricezione e l'elaborazione dei dati raccolti da servizi stranieri nell'ambito della cooperazione e trasmessi al Servizio di intelligence federale sono regolati dalle sezioni 14 f. BNDG non specificoLa ricezione e l'elaborazione dei dati raccolti da servizi stranieri nell'ambito della cooperazione e trasmessi al Servizio di intelligence federale sono regolati dalle sezioni 14 f. BNDG non specifico regolata.

13

5. Oltre alle presenti norme speciali in materia di raccolta, elaborazione, conservazione, cancellazione e trasmissione relative al chiarimento delle telecomunicazioni estere-estere, si applicano le disposizioni generali della legge sull'uso, l'elaborazione di BND, non modificate dalla modifica della legge del 23 dicembre 2016 , Archiviazione, correzione, cancellazione e trasmissione di dati personali disponibili presso il Servizio di intelligence federale (sezioni 19, 20, 24 BNDG). Successivamente, il Servizio di intelligence federale può salvare, modificare e utilizzare i dati personali provenienti dall'intelligence estera-straniera, nella misura in cui ciò è necessario per l'adempimento dei suoi compiti (Sezione 19 (1) BNDG). Deve correggerli ed eliminarli se non sono corretti o non sono più tenuti a svolgere le sue funzioni,I periodi di prova qui richiesti possono avere una durata massima di dieci anni (Sezione 20 (1) BNDG, Sezione 12 BVerfSchG). La Sezione 24 BNDG e le norme del Federal Constitution Protection Act cui si fa riferimento autorizzano il Servizio di intelligence federale a trasmettere le informazioni ottenute, in particolare i dati personali, a specifici organismi nazionali e stranieri in singoli casi.

14

6. I dettagli del processo di raccolta e trattamento, le responsabilità di controllo all'interno del servizio e il trasferimento dei dati nell'ambito delle cooperazioni devono essere regolati in regolamenti di servizio che richiedono l'approvazione della Cancelleria federale (Sezione 6 (7), Sezione 15 (3) Frase 5 BNDG). Oltre a questi requisiti legali, i dettagli tecnici e pratici dell'intero processo di raccolta e valutazione, la cooperazione e la trasmissione dei dati sono regolati da norme di servizio non pubblico. Al momento di decidere, il Senato era soggetto alla "Prestazione di servizi ai sensi della Sezione 6 (7) BNDG per la ricognizione strategica delle telecomunicazioni del BND (DV SIGINT)" - con annerimento isolato - la "Fornitura di servizi per la trasmissione di informazioni da parte del Servizio federale di intelligence (trasmissione DV)",il "Regolamento sui servizi per il profilo professionale del governo federale (DV APB)" e il "Regolamento sui servizi per la conclusione di accordi internazionali con servizi di intelligence esteri (DV International Agreement - AND)".

15

7. Prima che le competenze controverse fossero emesse e da allora in pratica, si è sviluppata una pratica di educazione strategica alle telecomunicazioni estere , che è divisa in diverse fasi.

16

a) Innanzitutto, il Servizio di intelligence federale accede ai flussi di dati di telecomunicazione intercettando i segnali dalle reti di telecomunicazione con i propri dispositivi o facendo instradare i flussi di dati dai fornitori di servizi di telecomunicazione conformemente alla sezione 8 BNDG. Questo si basa sulle disposizioni di rete della Cancelleria federale (Sezione 6 (1) frase 2; vedere il

paragrafo 10 sopra). Tre dei 17 accordi di rete attualmente in vigore riguardano nodi Internet situati in Germania. Le restanti disposizioni riguardano essenzialmente le reti satellitari.

17 °

Le reti organizzate dalla Cancelleria federale possono quindi in particolare essere indirizzate a specifici ordini di deviazione da parte del Servizio di intelligence federale verso i fornitori di servizi di telecomunicazione in conformità alla sezione 8 (1) frase 1 BNDG. La sezione 8 BNDG consente di rilevare le telecomunicazioni di linea in Germania sulla base di ordini di deviazione dal Servizio di intelligence federale indirizzati ai fornitori di servizi di telecomunicazione. Queste disposizioni sulla diversione sono di particolare importanza pratica. Secondo il governo federale, delle centinaia di hub Internet in tutto il mondo in cui le sottoreti che compongono Internet sono interconnesse, 27 si trovano in Germania, tra cui la più grande e più importante del mondo al momento DE-CIX a Francoforte sul Meno.

18

Nell'ambito di un accordo di rete della Cancelleria federale (sezione 6 (1) frase 2 BNDG), ma anche nell'ambito degli ordini di diversione che attuano parzialmente gli accordi di rete (sezione 8 (1) frase 1 BNDG), è possibile organizzare simultaneamente più reti per la registrazione, il che è anche pratico corrisponde. Spesso vengono organizzate in modo significativo più reti con una capacità di registrazione molto maggiore rispetto ai dati effettivamente richiamati. Secondo il governo federale in udienza, il servizio di intelligence federale accede effettivamente a una media di circa il dieci percento della capacità totale della rete ordinata per la registrazione al fine di elaborare e valutare i dati in essa contenuti.Nella misura in cui il Servizio di intelligence federale si avvale di fornitori di servizi di telecomunicazione che sono obbligati a cooperare in conformità con la Sezione 8 BNDG, le reti effettivamente monitorate sono selezionate in modo tale che il servizio sia trasferito dalle reti contenute nell'ordine di deviazione a singoli fornitori, sottoreti o oltre richieste di rotte di trasmissione tramite le cosiddette tabelle di stato (cfr. BVerwG, sentenza del 30 maggio 2018 - 6 A 3.16 -, punto 5). Secondo la dichiarazione scritta dell'associazione industriale eco - Verband der Internetwirtschaft eV, i sistemi tecnici del Servizio di intelligence federale installati presso l'hub Internet DE-CIX hanno attualmente la capacità di registrare ed elaborare circa il cinque percento del traffico delle telecomunicazioni attraversato qui.Le reti effettivamente monitorate sono selezionate in modo tale che il servizio richieda singole reti, sottoreti o collegamenti di trasmissione dalle reti contenute nell'accordo di diversione dal rispettivo fornitore tramite le cosiddette tabelle di stato per la diversione (vedi BVerwG, sentenza del 30 maggio 2018 - 6 A 3.16 -, paragrafo 5). Secondo la dichiarazione scritta dell'associazione industriale eco - Verband der Internetwirtschaft eV, i sistemi tecnici del Servizio di intelligence federale installati presso l'hub Internet DE-CIX hanno attualmente la capacità di registrare ed elaborare circa il cinque percento del traffico delle telecomunicazioni attraversato qui.Le reti effettivamente monitorate sono selezionate in modo tale che il servizio richieda singole reti, sottoreti o collegamenti di trasmissione dalle reti contenute nell'accordo di diversione dal rispettivo fornitore tramite le cosiddette tabelle di stato per la diversione (vedi BVerwG, sentenza del 30 maggio 2018 - 6 A 3.16 -, paragrafo 5). Secondo la dichiarazione scritta dell'associazione industriale eco - Verband der Internetwirtschaft eV, i sistemi tecnici del Servizio di intelligence federale installati presso l'hub Internet DE-CIX hanno attualmente la capacità di registrare ed elaborare circa il cinque percento del traffico delle telecomunicazioni attraversato qui.Richiede sottoreti o linee di trasmissione per le cosiddette tabelle di stato per il rifiuto (vedi BVerwG, sentenza del 30 maggio 2018 - 6 A 3.16 -, punto 5). Secondo la dichiarazione scritta dell'associazione industriale eco - Verband der Internetwirtschaft eV, i sistemi tecnici del Servizio di intelligence federale installati presso l'hub Internet DE-CIX hanno attualmente la capacità di registrare ed elaborare circa il cinque percento del traffico delle

telecomunicazioni attraversato qui.Richiede sottoreti o linee di trasmissione per le cosiddette tabelle di stato per il rifiuto (vedi BVerwG, sentenza del 30 maggio 2018 - 6 A 3.16 -, punto 5). Secondo la dichiarazione scritta dell'associazione industriale eco - Verband der Internetwirtschaft eV, i sistemi tecnici del Servizio di intelligence federale installati presso l'hub Internet DE-CIX hanno attualmente la capacità di registrare ed elaborare circa il cinque percento del traffico delle telecomunicazioni attraversato qui.I sistemi tecnici del Servizio di intelligence federale installati presso l'hub Internet DE-CIX hanno attualmente la capacità di registrare ed elaborare circa il cinque percento del traffico di telecomunicazioni passato qui.I sistemi tecnici del Servizio di intelligence federale installati presso l'hub Internet DE-CIX hanno attualmente la capacità di registrare ed elaborare circa il cinque percento del traffico di telecomunicazioni passato qui.

19

b) Con il trasferimento del flusso di dati reso accessibile dal trasferimento di dati o mediante altri metodi di intercettazione ai sistemi di acquisizione del Servizio di intelligence federale, inizia un processo di filtraggio e valutazione a più fasi e completamente automatizzato, che termina con la memorizzazione o la cancellazione dei dati temporaneamente memorizzati. I flussi di dati vengono prima preparati tecnicamente in modo da poter essere assegnati a diversi tipi di dati (ad es. Dati di streaming, dati di cronologia di Internet, dati di processi di telecomunicazione) e, se irrilevanti dal punto di vista tecnico, possono essere separati. Quindi i dati di telecomunicazione registrati vengono filtrati elettronicamente allo scopoRiconoscere ed eliminare il traffico di dati non soggetto alle indagini estere-straniere con la partecipazione di cittadini o residenti tedeschi (il cosiddetto filtro DAFIS). A tal fine, il traffico di telecomunicazioni registrato viene verificato per riferimento nazionale o tedesco utilizzando vari criteri formali relativi ai metadati (ad esempio l'uso di un dominio di primo livello tedesco) e inoltre confrontato con un elenco tenuto dal Federal Intelligence Service ("elenco positivo G 10") di codici di telecomunicazione assegnati a residenti o tedeschi può essere. Il grado di affidabilità di questo filtro è controverso, così come le attuali possibilità tecniche per un migliore filtraggio tra le parti coinvolte.Secondo il governo federale, gli indirizzi IP possono essere assegnati con precisione specifica per paese con una sicurezza del 98 percento. Al fine di riconoscere tale traffico di dati con la partecipazione di residenti o tedeschi, che possono essere assegnati solo a indirizzi IP stranieri a causa dell'interconnessione di server situati all'estero o dell'uso di hotspot, il servizio di intelligence federale include anche criteri e metadati formali aggiuntivi nel suo filtro. Il tasso di errore complessivo per la classificazione del traffico come puro traffico internazionale è sconosciuto.che, ad esempio a causa dell'interconnessione di server situati all'estero o dell'uso di hotspot, può essere assegnato solo a indirizzi IP stranieri, il servizio di intelligence federale include anche criteri e metadati formali aggiuntivi nel suo filtro. Il tasso di errore complessivo per la classificazione del traffico come puro traffico internazionale è sconosciuto.che, ad esempio a causa dell'interconnessione di server situati all'estero o dell'uso di hotspot, può essere assegnato solo a indirizzi IP stranieri, il servizio di intelligence federale include anche criteri e metadati formali aggiuntivi nel suo filtro. Il tasso di errore complessivo per la classificazione del traffico come puro traffico internazionale è sconosciuto.

20

Il governo federale sostiene che il numero di transazioni di telecomunicazione in cui il coinvolgimento di cittadini o residenti tedeschi non è inizialmente riconosciuto dai processi di filtro, ma è successivamente rivelato al Servizio di intelligence federale come parte di ulteriori valutazioni e utilizzo dei dati, è molto basso nella pratica. Nella valutazione manuale del traffico di telecomunicazioni selezionato dai termini di ricerca, in cui circa 270.000 traffico di contenuti giornalieri sarebbero ridotti a circa 260 messaggi pertinenti da un insieme di criteri diversi (sotto il margine 24 f.), In realtà era noto solo un traffico di telecomunicazioni al giorno, i cittadini nazionali

di cui - o il riferimento tedesco non è stato riconosciuto elettronicamente. Secondo il governo federale, finora è stato registrato solo un casoin cui è stata omessa la cancellazione di un traffico di telecomunicazioni successivamente riconosciuto relativo alla Germania o alla Germania con l'approvazione della Commissione G10 (§ 10 para.4 frasi da 2 a 6 BNDG).

21

c) Il Servizio di intelligence federale raccoglie e archivia i dati sul traffico rimanenti dopo il filtro DAFIS (Sezione 6 Paragrafo 6 Frase 1 BNDG), vale a dire indipendentemente dai selettori, e li valuta in un secondo momento principalmente utilizzando i dati del computer e altri metodi di analisi.

22

d) Il contenuto delle telecomunicazioni, d'altra parte, viene archiviato e valutato oltre l'archiviazione intermedia tecnicamente necessaria ai sensi della Sezione 6 Paragrafo 2 BNDG se elementi di telecomunicazioni registrati sono stati identificati durante il confronto controllato da computer con termini di ricerca precedentemente definiti (selettori) e separati dal flusso di dati come pertinenti . Secondo il governo federale e i requisiti del pertinente regolamento di servizio (DV SIGINT), i termini di ricerca utilizzati a tale scopo sono utilizzati internamente da una sotto-unità ("Quality Assurance SIGINT") prima dell'uso attivo ("controllo") per conformità dell'ordine, ammissibilità legale - in particolare per quanto riguarda la loro proporzionalità - e Plausibilità controllata. Catturato dai sistemi del Servizio di intelligence federale,ma i dati relativi al contenuto delle telecomunicazioni non selezionati sulla base dei termini di ricerca vengono eliminati dai sistemi di registrazione senza lasciare residui dopo il confronto.

23

I selettori distinguono tra contenuto e termini formali, in base ai quali il Servizio di intelligence federale utilizza prevalentemente (secondo il governo federale, circa il 90 percento) termini di ricerca formale. Queste sono funzioni di comunicazione, come ID di connessione o indirizzi e-mail, che possono essere assegnati a persone, entità, gruppi o fenomeni considerati rilevanti ai fini dell'intelligence. Utilizzando tali termini di ricerca, il Servizio federale di intelligence può identificare tutte le telecomunicazioni dai flussi di dati registrati e separarle per l'archiviazione diretta, originata o contenente l'identificatore o l'indirizzo utilizzato come termine di ricerca. Secondo il governo federale, circa il cinque percento dei termini di ricerca servono allo scopoacquisire conoscenze specifiche sugli individui in merito alle misure da adottare nei loro confronti; negli altri casi, le persone dietro i termini di ricerca controllata sono conosciute solo parzialmente, senza se stesse e il loro comportamento è al centro dell'interesse educativo.

24

In questo modo, il servizio di intelligence federale seleziona i dati di contenuto tra circa 270.000 processi di telecomunicazione giornalieri tra persone (e-mail, telefonata, messaggi di chat) dal volume di dati registrati utilizzando un numero di sei cifre di termini di ricerca e li memorizza per un'ulteriore valutazione manuale. Questa cifra è costituita dal traffico nazionale (circa il 60 percento) e da record stranieri (circa il 40 percento), nonché da un basso numero di cinque cifre del traffico di telecomunicazioni fornito al servizio dai servizi di intelligence stranieri che hanno collaborato. Inoltre, il servizio di intelligence federale raccoglie e archivia una quantità di dati sul traffico che è ogni giorno superiore di diversi ordini di grandezza.

25

e) La selezione e la memorizzazione del traffico di contenuti utilizzando i termini di ricerca è seguita da un'ulteriore valutazione. Al centro di questo passaggio c'è la valutazione manuale della rilevanza dell'intelligence. Qui, una media di circa 260 traffico di dati viene attualmente identificata su base giornaliera, che viene inoltrata alle "aree decrescenti". Secondo il governo federale, anche la protezione delle aree centrali secondo § 11 BNDG è praticamente implementata in questo contesto - insieme alla valutazione della pertinenza e all'ispezione manuale per un rilevamento accidentale di telecomunicazioni internazionali o nazionali. Al contrario, secondo il governo federale, i requisiti per la protezione delle aree centrali non hanno alcun effetto pratico per le precedenti fasi procedurali.Secondo la normativa ufficiale pertinente (DV SIGINT) e le informazioni del governo federale, la valutazione protetta delle persone autorizzate a rifiutare di testimoniare ai sensi dell'articolo 53 StPO è presa in considerazione nella valutazione manuale; In base a ciò, tale comunicazione può essere utilizzata solo se il particolare valore informativo del contenuto delle telecomunicazioni registrato supera gli interessi confidenziali di conflitto.

26

f) Per la prima volta, la pratica della cooperazione in materia di intelligence è regolata dalla legge nelle sezioni da 13 a 15 BNDG. Questo era l'obiettivo principale del lavoro di informazione in seno al comitato di indagine dell'NSA (cfr BTDrucks 18/12850, pagg. 516 e seguenti; 706 e seguenti; da 761 a 1007). Secondo i documenti legali (BTDrucks 18/9041, p. 29) e le informazioni fornite dal governo federale, gli obiettivi di questa pratica sono l'uso efficace delle risorse educative, l'espansione del database accessibile ai servizi nel loro insieme e il costante scambio di know-how di intelligence, in particolare competenze tecniche e termini di ricerca adeguati.

27

Di conseguenza, il servizio di intelligence federale utilizza un gran numero di termini di ricerca specificati dai servizi dei partner nel contesto delle cooperazioni, ma anche per la propria formazione in materia di telecomunicazioni. Ciò riguarda circa il 50-60 percento dei termini di ricerca che il Servizio di intelligence federale sta attualmente utilizzando per registrare. Tuttavia, il servizio non utilizza termini di ricerca il cui significato, funzionalità o tipo sono sconosciuti. Piuttosto, secondo le norme e le informazioni ufficiali pertinenti del governo federale, richiede ulteriori informazioni su ciascun termine di ricerca indicato da un servizio partner, che è integrato in un controllo elettronico dei termini di ricerca. Inoltre, controlla elettronicamente i termini di ricerca nominati dai servizi stranieri per un riferimento tedesco o nazionale prima che vengano utilizzati.per una violazione dei limiti delle registrazioni mirate in conformità con la Sezione 6 (3) BNDG, per una violazione degli interessi della Repubblica Federale Tedesca e per alcuni criteri formali definiti in relazione alla rispettiva cooperazione e ai suoi obiettivi. Inoltre, il servizio di intelligence federale effettua un numero minimo mensile di campioni manuali per ciascuna cooperazione, quella effettiva Secondo le proprie informazioni, il numero di campioni casuali va oltre quanto previsto dalle normative e interessa circa 300 termini di ricerca al mese.

28

Il filtraggio elettronico delle telecomunicazioni nazionali e internazionali offerto prima della trasmissione automatica in conformità alla sezione 15 (1) n. 1a BNDG viene effettuato in pratica secondo il modello sopra citato. Inoltre, vengono utilizzati metodi di filtraggio per separare tali registrazioni, la cui trasmissione porterebbe al timore di una violazione degli interessi tedeschi (Sezione 15 (1) n. 1b BNDG). Al fine di verificare la funzionalità di questi processi di filtraggio

automatico (Sezione 15 (3) BNDG), il Servizio federale di intelligence, secondo il governo federale, effettua nuovamente controlli in loco manuali in udienza, il cui numero minimo mensile è anche specificato nel regolamento di servizio per cooperazione e che in pratica è mensile copre circa 25 a 40 segnalazioni presentate.

29

La trasmissione di dati ai servizi dei partner in conformità con la sezione 15 (1) BNDG è inquadrata dalle restrizioni d'uso e dalle assicurazioni che devono essere previste nell'accordo di cooperazione in conformità con la sezione 13 (3) nn. 4-6 BNDG al fine di garantire la gestione dei dati della legge e la cancellazione dei dati. Il contenuto delle clausole da fornire di conseguenza nella dichiarazione di intenti è specificato dal pertinente regolamento ufficiale. Al fine di garantire che i dati vengano trattati in conformità con lo stato di diritto, il Servizio di intelligence federale fornisce a ogni singola trasmissione all'estero (Sezione 24 BNDG) un'aggiunta che contiene restrizioni e divieti di utilizzo, in conformità con le normative ufficiali pertinenti e le informazioni fornite dal governo federale.

30

8. Questi processi sono integrati in norme speciali e generali in materia di trasparenza, supervisione e controllo. Internamente, vi è inizialmente un obbligo di etichettatura per i dati raccolti (Sezione 10 (1) BNDG) e requisiti speciali di registrazione per l'elaborazione non consentita dei dati (Sezione 10 (6), Sezione 11 frase 4 BNDG) o trasmissione automatica a partner di cooperazione stranieri (Sezione 15 (2) BNDG). L'interessato ha diritto all'informazione, che tuttavia presuppone la presentazione di un interesse particolare e non si estende all'origine dei dati (sezione 22 BNDG). Gli obblighi di notifica sono previsti solo in caso di registrazione inammissibile e successiva memorizzazione dei dati delle telecomunicazioni con la partecipazione di residenti o tedeschi (Sezione 10 (4) frase 2 BNDG);non sono richieste notifiche per gli stranieri interessati all'estero, anche in caso di raccolta o trattamento di dati non ammessi.

31

La sezione 16 del BNDG istituisce il Comitato indipendente come un organo di controllo speciale, al quale i singoli poteri di controllo sono assegnati dalle sezioni da 6 a 15 del BNDG. Il Commissario federale per la protezione dei dati e la libertà delle informazioni è responsabile di un controllo generale sulla protezione dei dati (§§ 32, 32a BNDG). Un dipartimento della sua autorità è responsabile del controllo del Servizio di intelligence federale. Inoltre, la speciale responsabilità di controllo della Commissione G10 in caso di differimento di una comunicazione ai sensi della Sezione 10 (4) BNDG, il controllo parlamentare generale da parte dell'organismo di controllo parlamentare e del suo rappresentante permanente, nonché i poteri individuali che incidono su tale organo in relazione alle informazioni sulle telecomunicazioni estere-estere sono concessi (Sezione 6 (7) frase 3, Sezione 13 (5) frase 2 BNDG).

32

Secondo l'ex presidente del comitato indipendente e il responsabile federale della protezione dei dati, le attività di controllo di entrambi gli organismi sono praticamente limitate, citando i requisiti di riservatezza dei servizi cooperanti e gli accordi di riservatezza conclusi con essi ("norma di terzi").

II.

33

Con la loro denuncia costituzionale, i denuncianti lamentano una violazione del segreto delle telecomunicazioni ai sensi dell'articolo 10 GG. Nella misura in cui sono giornalisti, sostengono anche una violazione della libertà di stampa ai sensi dell'articolo 5, paragrafo 1, frase 2 della legge di base, poiché la legge BND per la sorveglianza strategica delle telecomunicazioni straniere non contiene alcuna regolamentazione speciale per proteggere il rapporto di fiducia tra la stampa e i suoi informatori contenere. Infine, i denuncianti 1) e i denuncianti da 3) a 5) lamentano una violazione del principio generale di uguaglianza ai sensi dell'articolo 3, paragrafo 1, GG perché non godono della stessa protezione dei tedeschi come persona giuridica o cittadino dell'UE residente in uno Stato membro.

34

1. In effetti, tutti i denuncianti affermano di essere interessati dalle autorizzazioni e dalle azioni del Servizio di intelligence federale basate su di loro nel contesto dell'educazione alle telecomunicazioni estero-straniera. Il denunciante di 1) è un'organizzazione non governativa con sede in Francia, che lavora a livello internazionale per la libertà di stampa e la sicurezza dei giornalisti contro le rappresaglie e in questo contesto fornisce anche a loro e ai loro parenti un aiuto concreto e personale concreto in situazioni problematiche (ad esempio in caso di detenzione o persecuzione) compie. Il denunciante 2) è in Azerbaigian e i denuncianti da 3) a 7) sono residenti in Germania, Regno Unito, Slovenia, Messico e Macedonia settentrionale,là e altrove giornalisti investigativi e giornalisti di nazionalità straniera, con denunciante 6) che lavorano per il dipartimento giornalistico di un'organizzazione non governativa messicana. Il denunciante di 8) è un cittadino tedesco residente in Guatemala che lavora come avvocato per un ufficio per i diritti umani e per la Commissione internazionale degli avvocati con sede a Ginevra.che lavora come avvocato per un ufficio per i diritti umani e per la Commissione di diritto internazionale con sede a Ginevra.che lavora come avvocato per un ufficio per i diritti umani e per la Commissione di diritto internazionale con sede a Ginevra.

35

Tutti i denuncianti affermano di utilizzare i servizi di telecomunicazione elettronica, in particolare la posta elettronica, il telefono e la messaggistica istantanea, in larga misura privatamente o nell'ambito delle loro attività professionali. Lavorerebbero regolarmente su argomenti e comunicheranno con le persone nelle regioni che, ovviamente, potrebbero attirare l'attenzione di un'istruzione di telecomunicazioni estera-straniera da parte del Servizio di intelligence federale. In particolare, i denuncianti 2) e i denuncianti da 3) a 7), in qualità di giornalisti investigativi, ottengono una parte significativa delle conoscenze richieste agli informatori con i quali hanno comunicato in larga misura utilizzando la tecnologia della comunicazione. Queste fonti sono spesso impiegati del governo o del settore privato,I parenti di organizzazioni illegali o le loro persone di contatto che, attraverso la loro partecipazione, si espongono spesso a rischi considerevoli. Il denunciante 1) e il denunciante 8) erano inoltre regolarmente in contatto con tali persone nel contesto delle loro attività legali o professionali.

36

2. Per quanto riguarda la ricevibilità, le ricorrenti sostengono che possono essere interessate da misure basate sui regolamenti impugnati. Dal momento che c'era già una fondamentale ingerenza nella registrazione dei dati di telecomunicazione associati al confronto dei termini di ricerca o alla memorizzazione dei dati sul traffico, dovresti solo dimostrare che è probabile che il Servizio di

intelligence federale venga registrato come parte dell'indagine di intelligence estera-straniera. Questo è il caso, come mostra un calcolo statistico di esempio, in considerazione della diffusione delle misure e dell'altissimo volume di telecomunicazioni di tutti i denuncianti. Anche se lo chiediErano in realtà preoccupati che le loro telecomunicazioni sarebbero state selezionate con una certa probabilità nel confronto dei termini di ricerca per ulteriori valutazioni, poiché le loro attività si riferiscono costantemente ad argomenti e aree in cui sarebbe evidente un maggiore interesse delle informazioni estere tedesche. Nonostante gli sforzi del Federal Intelligence Service per filtrare automaticamente la comunicazione con la partecipazione di residenti e tedeschi, il denunciante 8) è stato probabilmente influenzato dal chiarimento delle telecomunicazioni estero-straniere con una certa probabilità. Perché si può presumere che il Servizio di intelligence federale non lo consideri il funzionario di una persona giuridica straniera come una persona con diritti fondamentali.poiché le loro attività riguardano costantemente argomenti e settori in cui è evidente un crescente interesse per l'intelligence estera tedesca. Nonostante gli sforzi del Federal Intelligence Service per filtrare automaticamente la comunicazione con la partecipazione di residenti e tedeschi, il denunciante 8) è stato probabilmente influenzato dal chiarimento delle telecomunicazioni estero-straniere con una certa probabilità. Perché si può presumere che il Servizio di intelligence federale non lo consideri il funzionario di una persona giuridica straniera come una persona con diritti fondamentali.poiché le loro attività riguardano costantemente argomenti e settori in cui è evidente un crescente interesse per l'intelligence estera tedesca. Nonostante gli sforzi del Federal Intelligence Service per filtrare automaticamente la comunicazione con la partecipazione di residenti e tedeschi, il denunciante 8) è stato probabilmente influenzato dal chiarimento delle telecomunicazioni estero-straniere con una certa probabilità. Perché si può presumere che il Servizio di intelligence federale non lo consideri il funzionario di una persona giuridica straniera come una persona con diritti fondamentali.Nonostante gli sforzi del Federal Intelligence Service per filtrare automaticamente la comunicazione con la partecipazione di residenti e tedeschi, il denunciante 8) è stato probabilmente influenzato dal chiarimento delle telecomunicazioni estero-straniere con una certa probabilità. Perché si può presumere che il Servizio di intelligence federale non lo consideri il funzionario di una persona giuridica straniera come una persona con diritti fondamentali.Nonostante gli sforzi del Federal Intelligence Service per filtrare automaticamente la comunicazione con la partecipazione di residenti e tedeschi, il denunciante 8) è stato probabilmente influenzato dal chiarimento delle telecomunicazioni estero-straniere con una certa probabilità. Perché si può presumere che il Servizio di intelligence federale non lo consideri il funzionario di una persona giuridica straniera come una persona con diritti fondamentali.

37

Un'affermazione preventiva di un diritto all'informazione ai sensi del § 22 BNDG non è necessaria dal punto di vista della sussidiarietà, poiché questa affermazione registra solo i dati memorizzati e quindi nessuna informazione sulla raccolta, raccolta, conservazione temporanea o ulteriore elaborazione passata dei dati di telecomunicazione dei denuncianti sulla base di i regolamenti controversi. Precisazione e preparazione preventiva della controversia dinanzi ai tribunali specializzati, come richiesto in linea di principio dalla decisione della Corte costituzionale federale relativa alla registrazione delle targhe (BVerfGE 150, 309 <326 ff. Paragrafo 40 ss.>) Dal punto di vista della sussidiarietà,dati i limiti fattuali e legali della protezione legale dinanzi al Tribunale amministrativo federale, ciò non è possibile nelle costellazioni della sorveglianza strategica delle telecomunicazioni.

38

3. In quanto funzionari di una persona giuridica straniera, i denuncianti in riferimento ai punti 6) e 8) non erano esclusi dalla protezione dei diritti fondamentali ai sensi dell'articolo 10 GG. Anche i

funzionari di una persona giuridica straniera potrebbero avere diritti fondamentali. L'articolo 10.1 della Legge fondamentale protegge la riservatezza delle comunicazioni dai furti con scasso da parte dello Stato, indipendentemente dalla funzione in cui i partecipanti hanno comunicato. Inoltre, la comunicazione professionale e privata non poteva essere separata ex ante, poiché spesso anche le connessioni e gli indirizzi professionali venivano utilizzati privatamente.

39

4. I denuncianti da 1) a 7) sostengono inoltre che i diritti fondamentali denunciati - almeno nella loro dimensione del diritto della difesa - autorizzano anche gli stranieri all'estero ad affrontare le autorità statali tedesche. Questi diritti fondamentali non sono quelli che sono limitati ai tedeschi. Non si deve temere una collisione con il diritto internazionale riconoscendo un diritto fondamentale degli stranieri all'estero. Se non altro, il chiarimento delle telecomunicazioni estero-straniero viola il diritto internazionale, ma non il suo contenimento dei diritti fondamentali. La garanzia dei diritti fondamentali non è soggetta a una sottomissione speciale alla sovranità statale. Anche se segui questa tesi di compensazione,Nel caso di chiarimenti sulle telecomunicazioni estero-straniere, vi sarebbero rischi specifici, in particolare per gli stranieri all'estero, che giustificherebbero l'estensione ad essi dell'articolo 10 GG. In ogni caso, la separazione del traffico di telecomunicazioni nazionale e internazionale da quello delle telecomunicazioni puramente straniere è così incerta che la questione fondamentale della protezione dei diritti fondamentali non può essere significativamente subordinata da essa. Per i cittadini dell'Unione tra i denuncianti, esiste anche una ragione convincente per il riconoscimento dei diritti fondamentali dal divieto di discriminazione in base alla nazionalità ai sensi del diritto dell'Unione.In ogni caso, la separazione del traffico di telecomunicazioni nazionale e internazionale da quello delle telecomunicazioni puramente straniere è così incerta che la questione fondamentale della protezione dei diritti fondamentali non può essere significativamente subordinata da essa. Per i cittadini dell'Unione tra i denuncianti, esiste anche una ragione convincente per il riconoscimento dei diritti fondamentali dal divieto di discriminazione in base alla nazionalità ai sensi del diritto dell'Unione.In ogni caso, la separazione del traffico di telecomunicazioni nazionale e internazionale da quello delle telecomunicazioni puramente straniere è così incerta che la questione fondamentale della protezione dei diritti fondamentali non può essere significativamente subordinata da essa. Per i cittadini dell'Unione tra i denuncianti, esiste anche una ragione convincente per il riconoscimento dei diritti fondamentali dal divieto di discriminazione in base alla nazionalità ai sensi del diritto dell'Unione.

40

5. Alla luce dei diritti fondamentali degli stranieri all'estero, i regolamenti impugnati sono incostituzionali. Innanzitutto, stanno già violando l'obbligo di citazione ai sensi dell'articolo 19.1 frase 2 della Legge fondamentale. I regolamenti hanno inoltre interferito in modo sproporzionato con i loro diritti fondamentali. In considerazione del notevole grado di intervento della sorveglianza strategica che consente, i possibili obiettivi educativi sono insufficientemente limitati e importanti. In particolare, anche i limiti delle indagini mirate sono inadeguati e completamente assenti dai cittadini di paesi terzi. Alla luce delle informazioni talvolta altamente sensibili che possono essere generate dai dati sul traffico, l'autorità per raccoglierli èLa prenotazione e la valutazione non soggette a soglie o occasioni, in particolare per quanto riguarda le decisioni sulla conservazione dei dati della Corte di giustizia europea e della Corte costituzionale federale, non possono essere giustificate sulla base dei diritti fondamentali. A livello di valutazione, non esistono misure per proteggere speciali rapporti di riservatezza, in particolare di giornalisti e avvocati. Infine, ci sono notevoli deficit nell'area del controllo indipendente. Le responsabilità e il quadro di controllo dell'organismo indipendente sono troppo restrittivi. Inoltre, il controllo è suddiviso in modo disfunzionale tra organi diversi e nel complesso non è sufficientemente efficace per sostituire la

mancanza di fatto di protezione giuridica individuale. I poteri di trasferimento dei dati in singoli casi non erano aggiornati,soprattutto nella decisione della Corte costituzionale federale alla legge BKA (BVerfGE 141, 220). Ciò vale soprattutto per le loro soglie di trasmissione e le garanzie procedurali contro l'uso dei dati da parte del destinatario che è contrario allo stato di diritto. Le presunte carenze riguardano anche la cooperazione in materia di intelligence. In una forma maggiore, ciò si riferisce al trasferimento elettronico di dati ai servizi dei partner, nel contesto del quale le soglie di trasmissione sono state completamente eliminate. Dopotutto, il regime dell'educazione alle telecomunicazioni praticato dall'estero è solo estremamente rudimentale, incompleto e indefinito.

41

A sostegno della loro presentazione sulla mancanza di separabilità automatica delle telecomunicazioni nazionali, internazionali ed estere, i denuncianti hanno presentato una relazione tecnica, il cui contenuto adottano.

III.

42

Sul reclamo costituzionale sono state formulate le seguenti osservazioni: il governo federale, il governo dello stato bavarese, i rispettivi commissari federali per la protezione dei dati e la libertà di informazione e il sesto senato di revisione del tribunale amministrativo federale.

43

1. Il governo federale ha aderito al procedimento. In effetti, sottolinea la straordinaria importanza dell'educazione alle telecomunicazioni estere e straniere del Servizio di intelligence federale per fornire al governo federale le informazioni e le basi per il processo decisionale di cui ha bisogno. Da un punto di vista giuridico, considera la denuncia costituzionale irricevibile, ma in ogni caso infondata.

44

a) La comunicazione di intelligence estera da parte del Servizio di intelligence federale è di eccezionale importanza pubblica. Ciò vale tanto più in un mondo di nuove sfide della politica di sicurezza e di crescenti richieste e impegni da parte della Repubblica Federale come partner sovrano, economicamente forte e attivo a livello internazionale e integrato. Le informazioni sui paesi stranieri che possono essere ottenute mediante l'educazione alle telecomunicazioni straniere, autentiche, affidabili e indipendenti dagli interessi dei partner di cooperazione stranieri, spesso non possono essere ottenute da altre fonti di intelligence o possono essere ottenute solo con uno sforzo considerevolmente maggiore. Il processo di informazione del governo federale è controllato in modo completo.Una sorveglianza completa delle telecomunicazioni di determinate persone o regioni non è né prevista né possibile sullo sfondo del compito di informazione limitata e delle capacità tecniche del Servizio federale di informazione. Piuttosto, il Servizio di intelligence federale accede solo a una finestra infinitamente piccola nelle telecomunicazioni globali e concentra le sue capacità su obiettivi chiave relativi alla missione. Una specifica giuridica più dettagliata e un elenco finale dei possibili obiettivi delle informazioni estero-straniere, in particolare nel settore della cooperazione, non avrebbe senso, poiché mancherebbero la flessibilità e la gamma di argomenti necessarie.Allo stesso modo, una disposizione separata di ogni singolo termine di ricerca in una procedura formalizzata nell'area dell'educazione alle telecomunicazioni estere-straniere sullo sfondo

delle loro esigenze dinamiche e il numero di argomenti e paesi nel profilo professionale non è né immaginabile né utile. È inoltre essenziale mantenere disponibili i dati sul traffico non selezionati per un certo periodo di tempo, poiché confronti di posizione, reti o modelli di comportamento possono essere analizzati solo confrontandoli nel tempo e la capacità di chiarire rapidamente nuovi sviluppi ("capacità di avvio a freddo") richiede una certa quantità di dati disponibili.I processi tecnici di filtraggio automatico e cancellazione del traffico delle telecomunicazioni con la partecipazione di tedeschi o residenti vengono costantemente sviluppati e sono già altamente affidabili. Ad esempio, tutto il traffico IP che dovrebbe essere assegnato a un indirizzo IP che può essere localizzato in Germania verrebbe filtrato e scartato dal volume di dati registrati mediante il filtro del tipo IP. Successivamente, la comunicazione registrata viene automaticamente ricercata per un riferimento domestico o tedesco in base a ulteriori criteri formali (ad esempio l'uso di un cosiddetto dominio di primo livello tedesco) (livello DAFIS 1). Inoltre, tutte le telecomunicazioni registrate vengono automaticamente confrontate con un elenco positivo costantemente aggiornato e aggiornato (livello DAFIS 2),su cui si notano gli abbonati o gli ID di connessione che sono noti per essere assegnati a tedeschi o residenti ("elenco positivo G 10"). Inoltre, le telecomunicazioni nazionali o internazionali riconosciute come tali sono state successivamente risolte nell'ambito della valutazione manuale. Per quanto riguarda la cooperazione in materia di intelligence, il governo federale afferma che il Servizio federale di intelligence è assolutamente dipendente dalla cooperazione con i servizi di intelligence esteri per adempiere al proprio mandato. Nel fare ciò, deve anche rispettare la "Regola di terze parti", altrimenti i partner potrebbero essere risolti dai partner dell'intelligence.Inoltre, le telecomunicazioni nazionali o internazionali riconosciute come tali sono state successivamente risolte nell'ambito della valutazione manuale. Per quanto riguarda la cooperazione in materia di intelligence, il governo federale afferma che il Servizio federale di intelligence è assolutamente dipendente dalla cooperazione con i servizi di intelligence esteri per adempiere al proprio mandato. Nel fare ciò, deve anche rispettare la "Regola di terze parti", altrimenti i partner potrebbero essere risolti dai partner dell'intelligence.Inoltre, le telecomunicazioni nazionali o internazionali riconosciute come tali sono state successivamente risolte nell'ambito della valutazione manuale. Per quanto riguarda la cooperazione in materia di intelligence, il governo federale afferma che il Servizio federale di intelligence è assolutamente dipendente dalla cooperazione con i servizi di intelligence esteri per adempiere al proprio mandato. Nel fare ciò, deve anche rispettare la "Regola di terze parti", altrimenti i partner potrebbero essere risolti dai partner dell'intelligence.che il servizio di intelligence federale è assolutamente dipendente dalla cooperazione con i servizi di intelligence esteri. Nel fare ciò, deve anche rispettare la "Regola di terze parti", altrimenti i partner potrebbero essere risolti dai partner dell'intelligence.che il servizio di intelligence federale è assolutamente dipendente dalla cooperazione con i servizi di intelligence esteri. Nel fare ciò, deve anche rispettare la "Regola di terze parti", altrimenti i partner potrebbero essere risolti dai partner dell'intelligence.

45

b) Dal punto di vista giuridico, il governo federale considera già irricevibile la denuncia costituzionale. I denuncianti non avevano dimostrato che le misure basate sulle norme controverse avrebbero potuto essere interessate. Ciò vale anche se la probabilità di rilevamento da parte dei sistemi del Servizio di intelligence federale è sufficiente. Questo perché il servizio copre solo una parte trascurabile delle telecomunicazioni in tutto il mondo, quindi anche con un elevato volume di telecomunicazioni, è estremamente improbabile che vengano registrate le telecomunicazioni dei denuncianti, in particolare ulteriori elaborazioni e valutazioni. Consentono, come sostengono le ricorrenti,Se è sufficiente una connessione generale delle rispettive attività e comunicazioni con gli argomenti e le aree informative del Servizio di intelligence federale, la denuncia costituzionale nel settore delle informazioni straniere e straniere si trasformerebbe in una situazione popolare non intenzionale contro le leggi. Inoltre, i denuncianti non avevano fatto valere il diritto di accesso a un

reclamo costituzionale ai sensi della sezione 22 BNDG e non avevano intrapreso un'azione legale. Infine, la denuncia costituzionale era limitata nel tempo, poiché l'attuale prassi del Servizio di intelligence federale era stata esplicitamente standardizzata e limitata dai regolamenti impugnati. Almeno la limitazione si applica a tutte le normative,che - come le autorizzazioni di trasmissione - sarebbero esistite prima dell'emendamento controverso.

46

c) Il reclamo costituzionale è in ogni caso infondato. Ciò risulta già dalla mancanza di diritti fondamentali di tutti i denuncianti.

47

Per i denuncianti da 1) a 7), ciò deriva dal fatto che i diritti fondamentali denunciati a favore degli stranieri non forniscono protezione all'estero. La Corte costituzionale federale aveva espressamente lasciato aperta la questione della validità del segreto delle telecomunicazioni a favore degli stranieri all'estero nella sua decisione sulla sorveglianza strategica ai sensi dell'articolo 10 Act del 1999 (BVerfGE 100, 313). La questione dovrebbe essere trattata in modo differenziato e orientato a seconda dell'entità della responsabilità e della responsabilità delle autorità statali tedesche. Secondo il preambolo, i diritti fondamentali della Legge fondamentale sono fondamentalmente limitati al territorio e alle persone tedesche.La concessione di posizioni soggettive in materia di diritti fondamentali a favore degli stranieri all'estero costituisce presuntuoso potere legislativo straniero e viola il principio del diritto territoriale ai sensi del diritto internazionale. Al di là del territorio sovrano della Repubblica Federale, le persone che agiscono per il Servizio di Informazione Federale non affrontano i cittadini stranieri come sovranità. Quindi era logico non estendere loro il diritto fondamentale. L'estensione dei diritti fondamentali agli stranieri all'estero comporta anche il rischio di asimmetria di protezione, da allora i diritti di base, ma non il diritto di intervenire in base al principio territoriale, si estenderebbero a loro.Al di là del territorio sovrano della Repubblica Federale, le persone che agiscono per il Servizio di Informazione Federale non affrontano i cittadini stranieri come sovranità. Quindi era logico non estendere loro il diritto fondamentale. L'estensione dei diritti fondamentali agli stranieri all'estero comporta anche il rischio di asimmetria di protezione, da allora i diritti di base, ma non il diritto di intervenire in base al principio territoriale, si estenderebbero a loro.Al di là del territorio sovrano della Repubblica Federale, le persone che agiscono per il Servizio di Informazione Federale non affrontano i cittadini stranieri come sovranità. Quindi era logico non estendere loro il diritto fondamentale. L'estensione dei diritti fondamentali agli stranieri all'estero comporta anche il rischio di asimmetria di protezione, da allora i diritti di base, ma non il diritto di intervenire in base al principio territoriale, si estenderebbero a loro.ma non i poteri di intervento limitati a loro a livello nazionale secondo il principio territoriale.ma non i poteri di intervento limitati a loro a livello nazionale secondo il principio territoriale.

48

Per i denuncianti 6) e 8), la mancanza di preoccupazione per i diritti fondamentali derivava dal fatto che la loro posizione di funzionari di entità giuridiche straniere non poteva basarsi sui diritti fondamentali della Legge fondamentale. L'articolo 19.3 della Legge fondamentale concede espressamente i diritti fondamentali alle condizioni ivi specificate solo alle persone giuridiche nazionali. Poiché le persone giuridiche possono agire solo sulle persone fisiche come loro organi e rappresentanti, questa clausola relativa al segreto delle telecomunicazioni è vuota se le persone fisiche che agiscono e comunicano per persone giuridiche straniere in una funzione aziendale, in questo caso i denuncianti 6) e a 8), potrebbe invocare questo diritto fondamentale contro le misure di sorveglianza dello stato. Questo vale anchese l'ufficiale è tedesco.

49

d) Anche se si presume che i denuncianti abbiano diritti fondamentali, le disposizioni controverse sono costituzionali. Poiché l'intervento non sarebbe stato approfondito rispetto alla pratica legale precedente, il requisito di quotazione non era applicabile. Le regole sono sufficientemente specifiche, chiaramente definite e proporzionate alla luce dell'indispensabilità delle informazioni ottenute mediante l'educazione alle telecomunicazioni straniere. La profondità di intervento della ricognizione delle telecomunicazioni estero-straniere non è eccessiva alla luce del suo obiettivo, che si basa su informazioni generali e immagini della situazione, e del suo carattere non personale, ma reale. Una protezione procedurale dei diritti fondamentali con garanzie speciali in caso di registrazioni mirate sarà stabilita attraverso una procedura d'ordine più dettagliata.L'accesso alla sorveglianza del Servizio di intelligence federale è già soggetto a limiti considerevoli per motivi tecnici e di capacità, che contribuiscono alla proporzionalità del regolamento. Manca il riferimento alle decisioni della Corte costituzionale federale e della Corte di giustizia europea in merito alla conservazione dei dati, dal momento che non si tratta né di una documentazione completa né degli obiettivi dell'intelligence straniera comparabili con gli scopi della polizia preventiva. La richiesta di privilegi a favore di determinati gruppi professionali che vanno al di là della protezione delle aree centrali va oltre la giurisprudenza della Corte costituzionale federale, in base alla quale tali eccezioni non sono normalmente richieste nel settore della polizia preventiva.Il contenimento e la strutturazione aggiuntivi dell'attività di intelligence risulterebbero anche dalle norme di servizio pertinenti. La direzione e il controllo del Servizio di intelligence federale sono garantiti dal profilo professionale del governo federale e dall'interazione dei vari organi di controllo, in particolare dalla supervisione specialistica altamente sviluppata presso la Cancelleria federale.

50

2. Il governo dello stato bavarese sottolinea l'importanza della sicurezza politica della formazione delle telecomunicazioni estere e straniere e sostiene con un'ulteriore presentazione legale il ragionamento del governo federale in merito alla mancanza di diritti fondamentali degli stranieri all'estero. Secondo il suo preambolo, la Legge fondamentale non pretende di stabilire un ordine mondiale, ma limita piuttosto la sua validità al popolo tedesco e al territorio della Repubblica Federale. Inoltre, la Legge fondamentale distingue esplicitamente tra i diritti umani universali che devono essere considerati come pre-stato (art. 1 sec. 2 GG) e i "diritti fondamentali successivi". La dignità umana è stata preferita come base inalienabile di entrambe le clausole, che suggerisce sistematicamente una suggestione sistematica degli effetti dei diritti fondamentali al di fuori della Repubblica Federale.Dopotutto, è compito dei rispettivi ordinamenti giuridici stranieri proteggere le persone nel loro territorio nazionale dalla sorveglianza di altri stati che possono essere illegali secondo le norme ivi previste, che devono essere fatte valere dinanzi ai tribunali locali con i rispettivi rimedi legali. In ogni caso, la censura costituzionale è infondata, pertanto non vi è motivo di chiarire definitivamente la questione dei diritti fondamentali. A causa della natura automatizzata e precisamente non individualizzata delle misure, la natura intrusiva del chiarimento strategico delle telecomunicazioni è dubbia, ma in ogni caso ha un peso relativamente basso. I regolamenti impugnati hanno fornito una base giuridica sufficiente per questi interventi piuttosto minori.proteggere le persone sul loro territorio dalla sorveglianza di altri stati, che possono essere illegali secondo le norme ivi previste, che devono essere fatte valere dinanzi ai tribunali con i rimedi legali disponibili in ciascun caso. In ogni caso, la censura costituzionale è infondata, pertanto non vi è motivo di chiarire definitivamente la questione dei diritti fondamentali. A causa della natura automatizzata e precisamente non individualizzata delle misure, la natura intrusiva del chiarimento strategico delle telecomunicazioni è dubbia, ma in ogni caso ha un peso relativamente basso. I regolamenti impugnati hanno fornito una base giuridica sufficiente per questi interventi piuttosto minori.proteggere le persone sul loro territorio dalla sorveglianza di altri stati, che possono

essere illegali secondo le norme ivi previste, che devono essere fatte valere dinanzi ai tribunali locali con i rimedi legali disponibili. In ogni caso, la censura costituzionale è infondata, pertanto non vi è motivo di chiarire in modo conclusivo la questione dei diritti fondamentali. A causa della natura automatizzata e precisamente non individualizzata delle misure, la natura intrusiva della ricognizione strategica delle telecomunicazioni è dubbia, ma in ogni caso ha un peso relativamente basso. I regolamenti impugnati hanno fornito una base giuridica sufficiente per questi interventi piuttosto minori.cosa dovrebbe essere fatto valere dinanzi ai tribunali con i rimedi legali disponibili in ciascun caso. In ogni caso, la censura costituzionale è infondata, pertanto non vi è motivo di chiarire in modo conclusivo la questione dei diritti fondamentali. A causa della natura automatizzata e precisamente non individualizzata delle misure, la natura intrusiva della ricognizione strategica delle telecomunicazioni è dubbia, ma in ogni caso ha un peso relativamente basso. I regolamenti impugnati hanno fornito una base giuridica sufficiente per questi interventi piuttosto minori.cosa dovrebbe essere fatto valere dinanzi ai tribunali con i rimedi legali disponibili in ciascun caso. In ogni caso, la censura costituzionale è infondata, pertanto non vi è motivo di chiarire in modo conclusivo la questione dei diritti fondamentali. A causa della natura automatizzata e precisamente non individualizzata delle misure, la natura intrusiva della ricognizione strategica delle telecomunicazioni è dubbia, ma in ogni caso ha un peso relativamente basso. I regolamenti impugnati hanno fornito una base giuridica sufficiente per questi interventi piuttosto minori.A causa della natura automatizzata e precisamente non individualizzata delle misure, la natura intrusiva della ricognizione strategica delle telecomunicazioni è dubbia, ma in ogni caso ha un peso relativamente basso. I regolamenti impugnati hanno fornito una base giuridica sufficiente per questi interventi piuttosto minori.A causa della natura automatizzata e precisamente non individualizzata delle misure, la natura intrusiva del chiarimento strategico delle telecomunicazioni è dubbia, ma in ogni caso ha un peso relativamente basso. I regolamenti impugnati hanno fornito una base giuridica sufficiente per questi interventi piuttosto minori.

51

3. Il commissario federale per la protezione dei dati e la libertà di informazione - come il suo predecessore - critica in particolare l'inadeguata attuazione pratica dei requisiti di controllo costituzionale. Vi sono responsabilità parzialmente poco chiare e divise, non esistono opzioni sanzionatorie e mancano opzioni di scambio con altri organi di controllo. Vi sarebbero inoltre requisiti di informazione proattiva insufficienti e grandi asimmetrie di conoscenza nei confronti del Servizio di intelligence federale .Per quanto riguarda i dati ottenuti da altri servizi all'estero, il controllo della protezione dei dati è spesso impossibile perché il Servizio di intelligence federale nega l'accesso a tali dati, citando la "norma di terzi". In pratica, i reclami del commissario federale per la protezione dei dati sono stati ignorati senza la possibilità di portarli almeno al pubblico.

52

Vi sono inoltre notevoli preoccupazioni riguardo ai regolamenti impugnati, in particolare per quanto riguarda la loro certezza del diritto. In particolare, non vi è alcun obbligo di adattare costantemente i sistemi di filtro allo stato dell'arte attuale. Anche il regime di controllo oggettivo e indipendente è nel complesso inadeguato e in particolare non è adatto a sostituire la protezione giuridica giudiziaria che in realtà manca a causa della natura segreta delle misure in assenza di obblighi di notifica.

53

4. Il sesto senato di revisione del Tribunale amministrativo federale, che è responsabile della legge sulla sicurezza, dichiara di non essere stato direttamente interessato ai regolamenti controversi. Solo nel contesto dell'azione legale contro il fascicolo VERAS conservato in passato dal Servizio di

intelligence federale, il Senato ha trattato indirettamente il §§ 6 e seguenti BNDG e in particolare ha chiarito che i dati provenienti dal chiarimento delle telecomunicazioni estero-straniero a causa dell'esclusione dal § 6 Paragrafo 4, sezione 10 Paragrafo 4 BNDG per il file VERAS, che si applica anche ai residenti, non deve essere utilizzato. Una decisione sulla causa DE-CIX Management GmbH ricevuta dal Tribunale amministrativo federale nel marzo 2018 contro un ordine ai sensi della sezione 8 BNDG non era ancora prevedibile.

IV.

54

In vista dell'udienza, in risposta a un questionario della Corte costituzionale federale sulle circostanze tecniche delle reti di telecomunicazione internazionali e sulle possibilità e dimensioni del lavoro di intelligence del Servizio di intelligence federale, sono state rilasciate dichiarazioni scritte dal governo federale, il commissario federale per la protezione dei dati e la libertà di informazione, l'eco- Associazione dell'industria Internet, T-Systems International GmbH e Chaos Computer Club eV

55

Intervengono in udienza: i denuncianti, il governo federale, il servizio di intelligence federale, il pannello di controllo parlamentare, la commissione G10 e il commissario federale per la protezione dei dati e la libertà di informazione. L'ex funzionario della sicurezza informatica del governo Martin Schallbruch e il barrister e Queen's Counsel Dr. Tom Hickman, consigliere permanente presso il British Investigatory Powers Commissioner's Office. L'ex presidente del giudice indipendente presso la Corte di giustizia federale Gabriele Cirener, l'eco-associazione dell'industria Internet, T-Systems International GmbH e Chaos Computer Club eV sono stati ascoltati come terzi esperti.

B.

56

Il reclamo costituzionale è ricevibile.

IO.

57

Con la loro denuncia costituzionale legale, i denuncianti fanno appello contro i poteri di sorveglianza e trasmissione del Servizio di intelligence federale per la ricognizione delle telecomunicazioni estere. I loro attacchi sono diretti direttamente contro le norme dell'autorità che li autorizzano, ma indirettamente anche contro gli altri regolamenti con cui il legislatore ha affiancato questi poteri per garantirne la proporzionalità e senza i quali la loro costituzionalità non poteva essere valutata. Se la denuncia costituzionale viene interpretata in modo intelligente, i suoi attacchi si estenderanno inizialmente alle sezioni 6, 7 e alle sezioni da 13 a 15 del BNDG, per cui le sezioni da 9 a 11 e le sezioni 16, 20, 22, 32, 32a BNDG devono essere inclusi nell'esame;la questione viene quindi decisa sulla loro applicabilità e sostenibilità costituzionale come forma dei poteri contestati. Inoltre, i denuncianti si oppongono alla Sezione 19 (1) e alla Sezione 24 BNDG, comprese le altre disposizioni a cui si fa riferimento finora, nella misura in cui si applicano al trattamento dei dati dalla sorveglianza strategica in conformità alle Sezioni 6, 7, 13-15 BNDG Trova.

II.

58

I denuncianti sono autorizzati a presentare ricorso.

59

1. I denuncianti lamentano una violazione dei loro diritti fondamentali ai sensi dell'articolo 10 capoverso 1, dell'articolo 5 capoverso 1 frase 2 e dell'articolo 3 capoverso 1 GG. Sostengono che i regolamenti controversi hanno permesso loro di monitorare le telecomunicazioni, violando così il loro diritto fondamentale di mantenere il segreto delle telecomunicazioni. Nel fare ciò, spiegano più in dettaglio che il requisito di citazione dell'articolo 19.1 frase 2 della Legge fondamentale non era stato rispettato e che i regolamenti non soddisfacevano i requisiti di proporzionalità sotto vari aspetti. I denuncianti da 1) a 7) continuano a invocare una violazione del loro diritto fondamentale alla libertà di stampa dall'articolo 5, paragrafo 1, seconda frase, della legge di base, poiché le misure di sorveglianza potrebbero anche essere dirette contro di loro come giornalisti e non sono state prese misure di protezione a tale riguardo.Inoltre, il denunciante 1), in quanto entità giuridica di diritto privato residente nell'Unione europea, e il denunciante 3) e 5), in quanto cittadino dell'Unione, si oppongono al fatto di non essere esenti da tali misure di sorveglianza allo stesso modo dei cittadini e cittadini tedeschi. Vedi questo come una violazione dell'Art. 3 Par. 1 GG.

60

Con questa argomentazione, le possibili violazioni dei diritti fondamentali - basate sul contenuto della protezione fattuale - sono giustificate. Ciò vale non solo per la raccolta di dati, ma anche per l'uso e la trasmissione di dati, che devono essere misurati come interventi intrinseci ai diritti fondamentali rispetto ai diritti fondamentali che erano rilevanti per la raccolta dei dati (vedere BVerfGE 100, 313 <359 f.; 391>; 141, 220 <327 marginale 285>; stRspr).

61

2. Ai denuncianti da 1 a 7 non può essere negato il diritto di presentare ricorso perché, in quanto persona giuridica straniera o straniera residente all'estero, fanno affidamento sui diritti fondamentali della Legge fondamentale. Ad oggi, non è stato chiarito in modo definitivo se e in che misura i cittadini di altri paesi possano fare affidamento anche sui diritti fondamentali della Legge fondamentale in relazione alle misure delle autorità statali tedesche all'estero. Nella sua decisione del 14 luglio 1999, la Corte costituzionale federale non ha risposto positivamente né ha escluso (vedi BVerfGE 100, 313 <362 e seguenti>). In ogni caso, sembra possibile una violazione dei diritti fondamentali.

62

3. Il diritto di presentare ricorso non deve essere negato per la ricorrente 1) perché è una persona giuridica domiciliata all'estero. A tal fine, la denunciante afferma sufficientemente che l'estensione della protezione dei diritti fondamentali alle persone giuridiche dell'Unione europea può applicarsi a lei (a). Vi sono anche i prerequisiti per l'applicabilità essenziale ai sensi dell'articolo 19 capoverso 3 GG per i diritti fondamentali asseriti (b).

63

a) Su istanza dei trattati europei, la giurisprudenza della Corte costituzionale federale riconosce la possibilità di estendere la protezione dei diritti fondamentali alle persone giuridiche dell'Unione

europea. Le persone giuridiche con sede legale in un altro paese dell'UE sono trattate allo stesso modo delle persone giuridiche nazionali se la persona giuridica interessata dall'Unione europea agisce nell'ambito del diritto dell'Unione e se ha una connessione domestica sufficiente che applica i diritti fondamentali allo stesso modo di quelli nazionali rende necessarie le persone giuridiche (vedere BVerfGE 129, 78 <94 ss.>).

64

Successivamente, è almeno possibile un'estensione della protezione dei diritti fondamentali al denunciante in quanto persona giuridica straniera. Nella fattispecie, il denunciante 1) ha una connessione domestica che fa sorgere esigenze di protezione, che possono derivare dal fatto che i regolamenti impugnati consentono la sorveglianza all'interno del paese e dimostrano anche che le autorità tedesche sono interessate alle attività di persone controllate all'estero; questo pone anche la denunciante specificamente nel suo obiettivo di chiarimento.

65

Anche le attività del denunciante ai sensi dell'estensione dell'uso menzionate possono rientrare nell'ambito di applicazione del diritto dell'Unione. Ciò viene preso in considerazione, ad esempio, perché la denunciante si avvale delle sue libertà fondamentali garantite dal diritto primario accettando i servizi transfrontalieri nell'esercizio della sua libertà passiva di fornire servizi garantiti dall'articolo 56 TFUE. Tuttavia, in particolare la sicurezza nazionale rimane di esclusiva responsabilità dei singoli Stati membri ai sensi dell'articolo 4, paragrafo 2, frase 3, TUE, in modo che le azioni nell'ambito di applicazione del diritto dell'Unione possano essere escluse in ogni caso per quanto riguarda parti del profilo di compiti del Servizio federale di intelligence. Se e fino a che punto questo è il caso non è stato ancora chiarito ai sensi del diritto dell'UE (cfr.Domanda di pronuncia pregiudiziale proposta dall'Investigatory Powers Tribunal London [Regno Unito], presentata il 31 ottobre 2017, Privacy International, C-623/17, GU UE 2018 / C 022/41; Domanda di pronuncia pregiudiziale proposta dal Conseil d'État [Francia], presentata il 3 agosto 2018, La Quadrature du Net e a., C-511/18, GU UE 2018 / C 392/10 e French Data Network e a., C-512/18, GU UE 2018 / C 392/11 della direttiva 2002/58 / CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla protezione della vita privata nelle comunicazioni elettroniche - Direttiva sulla protezione dei dati per le comunicazioni elettroniche -, (GU UE 2002 / L 201/37, di seguito: RL 2002/58 / EG).GU UE 2018 / C 022/41; Domanda di pronuncia pregiudiziale proposta dal Conseil d'État [Francia], presentata il 3 agosto 2018, La Quadrature du Net e a., C-511/18, GU UE 2018 / C 392/10 e French Data Network e a., C-512/18, GU UE 2018 / C 392/11 della direttiva 2002/58 / CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla protezione della vita privata nelle comunicazioni elettroniche - Direttiva sulla protezione dei dati per le comunicazioni elettroniche -, (GU UE 2002 / L 201/37, di seguito: RL 2002/58 / EG).GU UE 2018 / C 022/41; Domanda di pronuncia pregiudiziale proposta dal Conseil d'État [Francia], presentata il 3 agosto 2018, La Quadrature du Net e a., C-511/18, GU UE 2018 / C 392/10 e French Data Network e a., C-512/18, GU UE 2018 / C 392/11 della direttiva 2002/58 / CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla protezione della vita privata nelle comunicazioni elettroniche - Direttiva sulla protezione dei dati per le comunicazioni elettroniche -, (GU UE 2002 / L 201/37, di seguito: RL 2002/58 / EG).Luglio 2002 sul trattamento dei dati personali e sulla protezione della vita privata nelle comunicazioni elettroniche - direttiva sulla protezione dei dati per le comunicazioni elettroniche -, (GU UE 2002 / L 201/37, di seguito: RL 2002/58 / EG).Luglio 2002 sul trattamento dei dati personali e sulla protezione della vita privata nelle comunicazioni elettroniche - direttiva sulla protezione dei dati per le comunicazioni elettroniche -, (GU UE 2002 / L 201/37, di seguito: RL 2002/58 / EG).

66

Se o in che misura il campo di applicazione del diritto dell'Unione sia stato effettivamente aperto non richiede una decisione sulla questione dell'ammissibilità della denuncia costituzionale. In ogni caso, il denunciante a 1) ha sottolineato la possibilità di una violazione di un diritto costituzionalmente conforme (vedere BVerfGE 125, 39 <73>; 129, 78 <91>). Non è richiesta una presentazione alla Corte di giustizia europea ai sensi dell'articolo 267, paragrafo 3, TFUE, poiché la denuncia costituzionale è comunque ammissibile; la domanda non è rilevante per la sostanza della decisione (si veda il margine 328 di seguito).

67

b) L'applicabilità essenziale dei diritti fondamentali rivendicati alle persone giuridiche, richiesta dall'articolo 19 capoverso 3 GG, è data per l'articolo 10 capoverso 1 GG, l'articolo 5 capoverso 1 frase 2 GG e l'articolo 3 capoverso 1 GG (vedere l'articolo 10.1 della Legge fondamentale: BVerfGE 100, 313 <356>; 106, 28 <43>; Articolo 5.1 della Legge fondamentale: BVerfGE 80, 124 <131>; 95, 28 <34 >; 113, 63 <75>; sull'articolo 3, paragrafo 1 GG: BVerfGE 21, 362 <369>; 42, 374 <383>; 53, 336 <345>).

68

4. Il diritto di appello dei denuncianti ai punti 6) e 8) non è inoltre escluso dal fatto che essi sono funzionari di persone giuridiche straniere che non sono loro stessi titolari di diritti fondamentali ai sensi dell'articolo 19.3 della Legge fondamentale.

69

Le persone che sostengono che i loro diritti fondamentali sono stati violati non sono escluse dalla protezione dei diritti fondamentali della Legge fondamentale perché agiscono come funzionari di una persona giuridica straniera (applicabile Hölscheidt, Jura 2017, p. 148 <153>; altrimenti, paragrafo 2.4 .5, 3.2.6 della prestazione di servizi ai sensi della Sezione 6 (7) BNDG per la ricognizione strategica delle telecomunicazioni del BND del 7 marzo 2019 [DV SIGINT]; Karl / Soiné, NJW 2017, p. 919 <920>; Dietrich, in: Schenke / Graulich / Ruthig [Ed.], Legge federale sulla sicurezza, 2a edizione 2019, § 6 BNDG Rn. 8 per funzionari di persone giuridiche con mansioni sovrane). I funzionari possono far valere i propri diritti di base, ma non come amministratore, hanno i diritti di base delle persone giuridiche per le quali agiscono.Tuttavia, per quanto riguarda i loro diritti fondamentali, la loro protezione non decade perché sono funzionari di una persona giuridica straniera che, a sua volta, non può fare affidamento sui diritti fondamentali della Legge fondamentale ai sensi dell'articolo 19.3 della Legge fondamentale (cfr. Hölscheidt, Jura 2017 , P. 148 <153>). Ciò vale anche se la protezione richiesta da loro avvantaggia anche la persona giuridica in singoli casi. In particolare, non è necessario revocare la protezione dei diritti fondamentali promessi a ciascun individuo come individuo al fine di evitare di compromettere l'articolo 19.3 GG. L'articolo 19.3 della legge di base non ha il compito di garantire l'adozione di misure sovrane contro soggetti giuridici stranieri,ma mira ad estendere la protezione individuale dei diritti fondamentali alle persone giuridiche. Se questa estensione è limitata alle persone giuridiche nazionali, ciò non riduce la protezione globale dei diritti fondamentali delle persone fisiche.

70

In base a ciò, anche i denuncianti di 6) e 8) sono autorizzati a presentare ricorso. Come gli altri denuncianti, fanno affidamento su una violazione dei loro diritti fondamentali ai sensi dell'articolo

10.1 della Legge fondamentale mediante la sorveglianza segreta delle loro telecomunicazioni sulla base dei regolamenti contestati. Il segreto delle telecomunicazioni dell'articolo 10, paragrafo 1 GG, come forma speciale di diritti personali generali e il diritto alla propria parola, mantiene la riservatezza della comunicazione individuale in quanto tale (cfr. BVerfGE 106, 28 <35 e seguenti>; Hermes, in: Dreier, GG, Vol.1, 3a edizione 2013, Art. 10 marg.15, 18). Non serve principalmente a proteggere il segreto materiale, ma a proteggere i singoli partecipanti alla comunicazione indipendentemente dal loro contenuto, dalle loro circostanze o dalla loro funzione (vedere BVerfGE 100, 313 <357>; 106, 28 <35 e seguenti>;vedi anche BVerfG, decisione della 3a camera del Primo Senato del 19 dicembre 1991 - 1 BvR 382/85 -, NJW 1992, p. 815 <816>). I diritti fondamentali dei denuncianti sono pertanto in discussione, la cui applicabilità non è influenzata dalle funzioni che svolgono per le persone giuridiche. Lo stesso vale per il denunciante a 6) nella misura in cui denuncia una violazione dell'articolo 5, paragrafo 1, frase 2 GG. Fa anche affidamento sulla protezione dei diritti fondamentali, che gli viene promesso come giornalista come persona ai sensi dell'articolo 5, paragrafo 1, frase 2 della legge fondamentale, indipendentemente dal fatto che lavori per una società di stampa o un'altra organizzazione (vedere BVerfGE 117, 244 < 258 ss.>).I diritti fondamentali dei denuncianti sono pertanto in discussione, la cui applicabilità non è influenzata dalle funzioni che svolgono per le persone giuridiche. Lo stesso vale per il denunciante a 6) nella misura in cui denuncia una violazione dell'articolo 5, paragrafo 1, frase 2 GG. Fa anche affidamento sulla protezione dei diritti fondamentali, che egli promette come giornalista direttamente come persona dall'articolo 5, paragrafo 1, frase 2 della Legge fondamentale, indipendentemente dal fatto che lavori per una società di stampa o un'altra organizzazione (vedere BVerfGE 117, 244 < 258 ss.>).I diritti fondamentali dei denuncianti sono pertanto in discussione, la cui applicabilità non è influenzata dalle funzioni che svolgono per le persone giuridiche. Lo stesso vale per il denunciante a 6) nella misura in cui denuncia una violazione dell'articolo 5, paragrafo 1, frase 2 GG. Fa anche affidamento sulla protezione dei diritti fondamentali, che gli viene promesso come giornalista come persona ai sensi dell'articolo 5, paragrafo 1, frase 2 della legge fondamentale, indipendentemente dal fatto che lavori per una società di stampa o un'altra organizzazione (vedere BVerfGE 117, 244 < 258 ss.>).Fa anche affidamento sulla protezione dei diritti fondamentali, che gli viene promesso come giornalista come persona ai sensi dell'articolo 5, paragrafo 1, frase 2 della legge fondamentale, indipendentemente dal fatto che lavori per una società di stampa o un'altra organizzazione (vedere BVerfGE 117, 244 < 258 ss.>).Fa anche affidamento sulla protezione dei diritti fondamentali, che gli viene promesso come giornalista come persona ai sensi dell'articolo 5, paragrafo 1, frase 2 della legge fondamentale, indipendentemente dal fatto che lavori per una società di stampa o un'altra organizzazione (vedere BVerfGE 117, 244 < 258 ss.>).

III.

71

I denuncianti sono direttamente, personalmente e attualmente interessati dai regolamenti impugnati. Il reclamo costituzionale soddisfa quindi direttamente i requisiti per i reclami costituzionali contro una legge.

72

1. I denuncianti non sono direttamente interessati. I poteri contestati devono essere attuati mediante ulteriori atti di esecuzione. Tuttavia, l'impatto diretto su una legge che richiede l'esecuzione può essere assunto anche se un denunciante non può intraprendere un'azione legale perché non è a conoscenza della misura o se è previsto un annuncio successivo, ma sarà anche evitato a lungo termine a causa di ampie eccezioni può essere (BVerfGE 150, 309 <324 Rn. 35> mwN; stRspr). Le misure di sorveglianza rese possibili dalla normativa impugnata sono sostanzialmente realizzate in

segreto. Gli obblighi di notifica successivi sono standardizzati dalla legge solo nel caso della sezione 10 (4) frase 2 BNDG,chi non riguarda i denuncianti da 1) a 7) in quanto cittadini stranieri e chi beneficia anche il denunciante 8) al massimo in casi eccezionali, vale a dire se una notifica non è nemmeno omessa (sezione 10, paragrafo 4, frase 5, del BNDG). La possibilità di ricevere informazioni sui dati memorizzati ai sensi del § 19 BNDG sulla tua persona ai sensi del § 22 BNDG in combinato disposto con il § 15 BVerfSchG non significa che il reclamo non venga immediatamente omesso, poiché queste norme non garantiscono che l'interessato sia interessato dalla La conoscenza acquisisce conoscenza (vedere BVerfGE 150, 309 <324 f. Margine n. 36>). Di norma, anche le persone interessate non sono a conoscenza dell'ulteriore uso o trasmissione dei dati consentiti dai regolamenti impugnati.Per questo motivo, i denuncianti non dovrebbero essere invitati ad attendere atti di esecuzione e ad agire contro di loro.

73

2. I denuncianti sono essi stessi e attualmente interessati dai regolamenti impugnati.

74

a) Dimostrate di essere probabilmente influenzato da misure per fornire informazioni all'estero a causa delle vostre attività di giornalista, attivista per i diritti civili e umani o come avvocato all'estero. Nel corso del loro lavoro, fanno affidamento sul fatto che comunicano ripetutamente con informatori che spesso rimangono nascosti e che, a loro conoscenza, il Servizio di intelligence federale ovviamente ha anche un notevole interesse in vista dei suoi compiti. Alla luce dell'ampia gamma di misure aperte dai regolamenti impugnati, che non sono adattate fin dall'inizio a un gruppo limitato di persone, viene dimostrata una probabilità sufficiente del loro attuale impatto sui propri diritti (vedi BVerfGE 109, 279 <307 f.>; 113, 348 < 363 f.>; 133,277 <312 f. Marg. 86 f.>; 141, 220 <262 marg. 84>). Alla luce dell'autorizzazione deliberatamente aperta, che ha lo scopo di consentire un adattamento flessibile alle esigenze di informazione della politica estera e di sicurezza del governo federale, non è improbabile che vengano toccati i settori di attività dei denuncianti. In considerazione della sorveglianza della comunicazione sospetta e confidenziale e delle misure di follow-up che stanno anche avvenendo in segreto, non è possibile richiedere ulteriori specifiche della presentazione (cfr. BVerfGE 100, 313 <356>).un tocco sulle aree di attività dei denuncianti non è remoto. In considerazione della sorveglianza della comunicazione sospetta e confidenziale e delle misure di follow-up che stanno anche avvenendo in segreto, non è possibile richiedere ulteriori specifiche della presentazione (cfr. BVerfGE 100, 313 <356>).un tocco sulle aree di attività dei denuncianti non è remoto. In considerazione della sorveglianza della comunicazione sospetta e confidenziale e delle misure di follow-up che stanno anche avvenendo in segreto, non è possibile richiedere ulteriori specifiche della presentazione (cfr. BVerfGE 100, 313 <356>).

75

b) Al momento il denunciante 8), in quanto cittadino tedesco, è preoccupato. Una raccolta di dati provenienti dal traffico delle telecomunicazioni da parte di cittadini tedeschi, di persone giuridiche nazionali o di persone residenti nel territorio federale è inammissibile ai sensi del § 6 Abs. 4 BNDG. Tuttavia, secondo il regolamento stabilito nella Sezione 10 (4) BNDG, il legislatore presuppone già che il filtraggio non garantisca sempre che la comunicazione di tali persone sia esclusa e che i dati possano essere raccolti in singoli casi contrariamente alla Sezione 6 (4) BNDG. Anche il governo federale ha dichiaratoche il traffico di telecomunicazioni registrato può essere riconosciuto come comunicazione tra tedeschi o cittadini tedeschi in base alla conoscenza individuale dei dipendenti del Servizio di intelligence federale. Questo riconoscimento viola i diritti fondamentali (vedi BVerfGE 150, 244 <266 para. 45>).

76

Indipendentemente da ciò, una preoccupazione attuale deriva dal fatto che il denunciante 8) secondo l'opinione legale del Servizio di intelligence federale stabilita nel regolamento di servizio, anche se tedesco, nel presente caso non ha alcuna protezione dei diritti fondamentali - e quindi non protegge § 6 para 4 BNDG - dovrebbe essere assegnato. Mentre lavora come avvocato in un ufficio per i diritti umani guatemalteco contro la sorveglianza, il Servizio di intelligence federale, come proposto dal governo federale, lo vede come un funzionario di una persona giuridica straniera che in quanto tale non può fare affidamento sui diritti fondamentali della Legge fondamentale. Il denunciante,che, per conto di questo ufficio, si occupa di aree che hanno diversi punti di contatto con possibili interessi di intelligence del Servizio di intelligence federale interessato dai regolamenti impugnati allo stesso modo dei denuncianti da 1) a 7).

IV.

77

La denuncia costituzionale soddisfa i requisiti di sussidiarietà.

78

1. Secondo il principio di sussidiarietà, tutti i mezzi che possono porre rimedio alla presunta violazione dei diritti fondamentali devono essere adottati prima che siano presentate le denunce costituzionali. I rimedi legali che possono essere ragionevoli a questo proposito possono includere la presentazione di un'azione dichiarativa o di ingiunzione, che consente chiarimenti legali specialistici su questioni di fatto o legali relative al processo decisionale (cfr. . La situazione è diversa, tuttavia, in quanto è solo una questione di limiti costituzionali per l'interpretazione degli standard. Nella misura in cui la valutazione di una norma solleva solo questioni costituzionali specifiche a cui la Corte costituzionale federale deve rispondere,Senza una migliore base decisionale prevista da un precedente controllo giudiziario specialistico, non è richiesta una precedente decisione giudiziaria specialistica (vedere BVerfGE 123, 148 <172 f.>; 143, 246 <322 marginale 211>; stRspr). A questo proposito, rimane che i reclami costituzionali direttamente contro una legge sono in gran parte ammissibili anche senza un ricorso preventivo ai tribunali specializzati (vedi BVerfGE 150, 309 <326 f. Rn. 44>).309 <326 f. Marg. 44>).309 <326 f. Marg. 44>).

79

2. Successivamente, i denuncianti non dovevano prima chiedere protezione legale a un giudice. La denuncia costituzionale, che è diretta direttamente contro le norme della legge sul Servizio di intelligence federale, solleva essenzialmente solo questioni costituzionali specifiche a cui la Corte costituzionale federale deve rispondere, senza una base sostanzialmente migliorata per il processo decisionale previsto da un precedente esame specialistico. Ciò si applica in ogni caso alla questione centrale del presente procedimento se i richiedenti come stranieri all'estero possano fare affidamento sui diritti fondamentali della Legge fondamentale in merito alle misure di sorveglianza. Ciò vale anche per l'esame dettagliato delle norme contestate.La tua valutazione costituzionale non dipende dall'interpretazione legale più dettagliata dei singoli elementi della base di attacco, ma dalla sostenibilità costituzionale della sorveglianza strategica delle telecomunicazioni in quanto tale e dalla sua sufficiente limitazione e certezza. Ciò non è diverso per le norme sulla raccolta e l'elaborazione dei dati rispetto alle norme sulla cooperazione con altri servizi. Anche per quanto riguarda le norme sulla trasmissione dei dati, la valutazione costituzionale non dipende in gran parte

dai dettagli dell'interpretazione, ma dal fatto che siano legalmente concepiti come tali in modo da soddisfare i requisiti costituzionali.ma piuttosto sulla sostenibilità costituzionale della sorveglianza strategica delle telecomunicazioni in quanto tale e la sua sufficiente limitazione e certezza. Ciò non è diverso per le norme sulla raccolta e l'elaborazione dei dati rispetto alle norme sulla cooperazione con altri servizi. Anche per quanto riguarda le norme sulla trasmissione dei dati, la valutazione costituzionale non dipende in gran parte dai dettagli dell'interpretazione, ma dal fatto che siano legalmente concepiti come tali in modo da soddisfare i requisiti costituzionali.ma piuttosto sulla sostenibilità costituzionale della sorveglianza strategica delle telecomunicazioni in quanto tale e la sua sufficiente limitazione e certezza. Ciò non è diverso per le norme sulla raccolta e l'elaborazione dei dati rispetto alle norme sulla cooperazione con altri servizi. Anche per quanto riguarda le norme sulla trasmissione dei dati, la valutazione costituzionale non dipende in gran parte dai dettagli dell'interpretazione, ma dal fatto che siano legalmente concepiti come tali in modo da soddisfare i requisiti costituzionali.Anche per quanto riguarda le norme sulla trasmissione dei dati, la valutazione costituzionale non dipende in gran parte dai dettagli dell'interpretazione, ma dal fatto che siano legalmente concepiti come tali in modo da soddisfare i requisiti costituzionali.Anche per quanto riguarda le norme sulla trasmissione dei dati, la valutazione costituzionale non dipende in gran parte dai dettagli dell'interpretazione, ma dal fatto che siano legalmente concepiti come tali in modo da soddisfare i requisiti costituzionali.

80

Inoltre, in base all'attuale stato delle sentenze amministrative, la protezione giuridica in tal senso non sarebbe neppure realizzabile. Il Tribunale amministrativo federale ha dichiarato inammissibili i reclami relativi al chiarimento strategico sulle telecomunicazioni, poiché l'attore non era in grado di designare un'azione sufficientemente specifica da parte del Servizio di intelligence federale (vedi BVerwGE 157, 8 <12 f. Margine 16 e seguenti>; 161, 76 <78 Paragrafo 14>); non è evidente che i denuncianti avrebbero potuto soddisfare questi requisiti qui.

V.

81

Infine, la denuncia costituzionale rispetta la scadenza per la presentazione di una denuncia ai sensi della Sezione 93 (3) BVerfGG.

82

1. La denuncia costituzionale presentata il 19 dicembre 2017 è conforme al periodo di legge di un anno nella misura in cui è diretta contro le disposizioni in base alle quali il legislatore federale regola i poteri del Servizio di intelligence federale per il chiarimento delle telecomunicazioni estere e straniere e per la cooperazione nell'ambito dell'intelligence delle telecomunicazioni estere-straniere per la prima volta ha. Le pertinenti disposizioni delle sezioni 6 e seguenti e delle sezioni 13 e seguenti BNDG sono conformi all'articolo 5 della legge sull'applicazione delle telecomunicazioni straniera e straniera del servizio di intelligence federale del 23 dicembre 2016 il giorno successivo alla promulgazione della legge, vale a dire il 31 dicembre 2016, entrato in vigore. Il fatto che il legislatore abbia collegato la prassi di intelligence esistente del Servizio federale di intelligence al nuovo regolamento non porta a spostare l'inizio della scadenza.L'oggetto del reclamo costituzionale non sono gli specifici atti di esecuzione del Servizio di intelligence federale, ai quali si applica il regolamento sui termini della sezione 93 (1) frase 1 BVerfGG; Piuttosto, è diretto contro l'autorizzazione legale a effettuare chiarimenti sulle telecomunicazioni estere come tali, per i

quali il periodo di reclamo della Sezione 93 (3) BVerfGG non inizia prima dell'entrata in vigore della legge.

83

2. Anche per quanto riguarda la Sezione 19 (1) BNDG e la Sezione 24 (1) a (3) BNDG, che regolano i poteri del Servizio di intelligence federale di archiviare, modificare e utilizzare o trasmettere dati personali, il periodo per presentare un reclamo è la Sezione 93 (3) BVerfGG mantenuto. Con l'entrata in vigore delle sezioni 6 e seguenti e delle sezioni 13 e seguenti BNDG, la portata di queste competenze generali di trasmissione ed elaborazione è stata estesa alle nuove misure regolamentate e quindi parzialmente ampliata. Questa è una nuova denuncia sui diritti fondamentali, per la quale è stato riavviato il periodo di denuncia (vedere BVerfGE 45, 104 <119>; 100, 313 <356>; 141, 220 <262 f. Rn. 85>; stRspr).

VI.

84

Poiché l'intelligence delle telecomunicazioni estere non è in ogni caso l'attuazione del diritto dell'Unione obbligatorio, la valutazione costituzionale della validità dei regolamenti impugnati si basa sui diritti fondamentali della legge di base. Ciò apre la giurisdizione della Corte costituzionale federale e la denuncia costituzionale è ammissibile a questo proposito. Ciò vale indipendentemente dal fatto che si possano applicare anche i diritti fondamentali dell'Unione (cfr. VerfG, decisione del Primo Senato del 6 novembre 2019 - 1 BvR 16/13 -, punto 39 - diritto all'oblio I).

85

Ciò non influisce sulla questione se ulteriori requisiti giuridici derivino direttamente dal diritto derivato dell'Unione europea, in particolare dall'articolo 15, paragrafo 1, della direttiva 2002/58 / CE per quanto riguarda la portata degli obblighi imposti ai fornitori di telecomunicazioni. L'interpretazione e l'applicazione del diritto specializzato dell'Unione Europea non è di competenza della Corte costituzionale federale, ma è per i tribunali specializzati in collaborazione con la Corte di giustizia europea (cfr. BVerfGE 148, 40 <48 f. Rn. 22>).

C.

86

La denuncia costituzionale è fondata. Le disposizioni contestate devono essere misurate rispetto ai diritti fondamentali della Legge fondamentale e intervenire nell'Articolo 10 Paragrafo 1 e nell'Articolo 5 Paragrafo 1 Frase 2 GG (da I a III). L'interferenza non è giustificata perché i regolamenti impugnati sono formalmente incostituzionali (sotto D). Inoltre, non soddisfano i requisiti materiali fondamentali dell'articolo 10 capoverso 1 e dell'articolo 5 capoverso 1 frase 2 GG (sotto E).

IO.

87

I diritti fondamentali della Legge fondamentale vincolano il Servizio di intelligence federale e il legislatore che ne disciplina i poteri indipendentemente dal fatto che il servizio sia attivo in

Germania o all'estero. La protezione dell'articolo 10 capoverso 1 e dell'articolo 5 capoverso 1 frase 2 GG si applica anche alla sorveglianza delle telecomunicazioni degli stranieri all'estero.

88

1. L'articolo 1, paragrafo 3, della legge fondamentale stabilisce un legame globale tra l'autorità statale tedesca e i diritti fondamentali della legge fondamentale. I requisiti restrittivi che subordinano il vincolo dei diritti fondamentali a una relazione territoriale con il territorio federale o l'esercizio di specifici poteri sovrani non possono essere trovati nel regolamento. In ogni caso, ciò si applica ai diritti fondamentali come diritti di difesa contro le misure di sorveglianza, come in discussione qui.

89

a) Ai sensi dell'articolo 1, sezione 3 della Legge fondamentale, i diritti fondamentali sono vincolanti per la legge, il potere esecutivo e la giurisprudenza come legge direttamente applicabile. Il regolamento non contiene restrizioni al territorio nazionale. Per le azioni degli enti statali tedeschi all'estero, un'eccezione alla validità dei diritti fondamentali non può essere derivata da una comprensione di base non espressa e concordata quando è stata istituita la Legge fondamentale (aA Hecker, in: Dietrich / Eiffler [ed.], Handbuch des Rechts der Nachrichtendienste, 2017, III Sezione 2, margine n. 46; Loffelmann, in: Dietrich / Eiffler [ed.], Handbuch des Rechts der Nachrichtendienste, 2017, VI Sezione 3 margine n. 15. In risposta al regime nazionalsocialista di violenza e arbitrarietà, l'articolo 1, paragrafo 3, GG mirava piuttosto a una visione globale,vincolo dei diritti fondamentali radicato nella dignità umana ed era già incorporato nella convinzione nel 1949 che la Repubblica Federale dovesse trovare il suo posto nella comunità internazionale come partner dello stato di diritto (cfr. Dreier, in: ders., GG, Vol. 1, 3a edizione 2013, Art. 1 paragrafo 2 marg.3; ders., DVBl 1999, p. 667 <672 segg.>). Ciò si riflette già nel preambolo, in particolare nell'articolo 1, paragrafo 2, GG e negli articoli 24 e 25 GG. Anche se il vincolo dei diritti fondamentali al di fuori del territorio del paese non era ancora una questione propria nelle deliberazioni sulla Legge fondamentale e, in particolare, le misure di sorveglianza nei confronti di paesi stranieri nelle forme oggi possibili erano al di là delle idee del tempo, non si può dedurre dalla storia di origine che la protezione dei diritti fondamentali fin dall'inizio dovrebbe finire al confine di stato.L'affermazione di una protezione globale dei diritti fondamentali, che mette le persone al centro, parla piuttosto del fatto che i diritti fondamentali dovrebbero sempre proteggere quando lo stato tedesco agisce e può quindi potenzialmente innescare esigenze di protezione, indipendentemente da dove e con chi.

90

b) Il vincolo ai diritti fondamentali secondo l'articolo 1 Paragrafo 3 GG come diritti di difesa individuale non si limita anche alle costellazioni in cui lo stato agisce come potere sovrano con il monopolio sull'uso della forza (cfr. Hölscheidt, Jura 2017, p. 148 < 150 f.>; AA Gärditz, Die Verwaltung 48 <2015>, p. 463 <474>; ders., DVBl 2017, p. 525 <526>; Hecker, in: Dietrich / Eiffler [ed.], Handbuch des Rechts der Nachrichtendienste, 2017, III § 2 Rn.46; Loffelmann, in: Dietrich / Eiffler [Ed.], Handbuch des Nachrichtendienst, 2017, VI § 3 Rn. 15). Tale restrizione, che preclude in gran parte un diritto fondamentale all'intelligence straniera, non può essere derivato, in particolare, dal fatto che l'articolo 1, paragrafo 3, GG non si riferisce all'autorità statale tedesca in quanto tale, ma piuttosto alla legislazione,il potere esecutivo e la giurisprudenza sono designati come diverse funzioni statali. Ciò non limita il vincolo dei diritti fondamentali, ma chiarisce piuttosto che la protezione dei diritti fondamentali si applica a tutti i poteri statali noti nella teoria tradizionale della separazione dei poteri, in particolare al legislatore, che all'epoca non era una cosa

ovvia (vedi Denninger, in: AK-GG, 2a edizione 1989) , Art. 1 cpv. 2, 3 marginali 17). Questo per garantire che tutti i rami della violenza di stato siano vincolati a tutti i diritti fondamentali (vedi Herdegen, in: Maunz / Dürig, GG, Art. 1 Par. 3 Paragrafo 12 [ottobre 2019]) è stata la base della formulazione originale dello standard, che è stata tradotta in "Legislazione, Amministrazione e giurisprudenza "ha imposto i tre poteri classici ai diritti fondamentali come legge direttamente applicabile.Con la sostituzione del termine "amministrazione" con il termine "potere esecutivo" con la legge che modifica la Legge fondamentale del 19 marzo 1956 (BGBl I p. 111), non era prevista alcuna restrizione al vincolo dei diritti fondamentali all'esercizio di specifici poteri sovrani. Piuttosto, il termine 1956 è stato ulteriormente considerato nel contesto dell'emendamento alla Legge fondamentale sulla costituzione militare rispetto al termine originale "amministrazione" e usato al suo posto per chiarire che la Bundeswehr si impegna anche a diritti fondamentali (BTDrucks 2/2150, p. 2) . Ciò non limita il vincolo dei diritti fondamentali alle decisioni che l'esecutivo potrebbe anche applicare con poteri sovrani.111) non intendeva limitare il vincolo dei diritti fondamentali all'esercizio di specifici poteri sovrani. Piuttosto, il termine 1956 è stato ulteriormente considerato nel contesto dell'emendamento alla Legge fondamentale sulla costituzione militare rispetto al termine originale "amministrazione" e usato al suo posto per chiarire che la Bundeswehr si impegna anche a diritti fondamentali (BTDrucks 2/2150, p. 2) . Ciò non limita il vincolo dei diritti fondamentali alle decisioni che l'esecutivo potrebbe anche applicare con poteri sovrani.111) non intendeva limitare il vincolo dei diritti fondamentali all'esercizio di specifici poteri sovrani. Piuttosto, il termine 1956 è stato ulteriormente considerato nel contesto dell'emendamento alla Legge fondamentale sulla costituzione militare rispetto al termine originale "amministrazione" e usato al suo posto per chiarire che la Bundeswehr si impegna anche a diritti fondamentali (BTDrucks 2/2150, p. 2) . Ciò non limita il vincolo dei diritti fondamentali alle decisioni che l'esecutivo potrebbe anche applicare con poteri sovrani.che la Bundeswehr si impegna anche per i diritti fondamentali (BTDrucks 2/2150, p. 2). Ciò non limita il vincolo dei diritti fondamentali alle decisioni che l'esecutivo potrebbe anche applicare con poteri sovrani.che la Bundeswehr è anche impegnata in diritti fondamentali (BTDrucks 2/2150, p. 2). Ciò non limita il vincolo dei diritti fondamentali alle decisioni che l'esecutivo potrebbe anche applicare con poteri sovrani.

91

Piuttosto, i diritti fondamentali vincolano la violenza dello stato in modo completo e nel suo insieme, indipendentemente da determinate funzioni, forme di azione o oggetti di performance statale (cfr. Hölscheidt, Jura 2017, p. 148 <150 f.>). La comprensione della violenza di stato è ampia e non si estende solo a misure imperative o sostenute da poteri sovrani. Tutte le decisioni che possono essere prese ai rispettivi livelli decisionali statali per essere autorizzate a essere prese per conto di tutti i cittadini sono coperte dai diritti fondamentali vincolanti. Ciò include misure, dichiarazioni e azioni di tipo sovrano e non sovrano: violenza di Stato vincolata a diritti fondamentali ai sensi dell'articolo 1, par.3 GG indica qualsiasi atto di organi o organizzazioni statali, poiché è svolto nell'esercizio del suo mandato impegnato per il bene comune (BVerfGE 128, 226 <244>). Il legame con i diritti fondamentali e la responsabilità decisionale politica sono indissolubilmente legati (vedi BVerfG, decisione del Primo Senato del 6 novembre 2019 - 1 BvR 16/13 -, punto 42 - diritto all'oblio I).

92

c) Il vincolo dei diritti fondamentali da parte delle potenze statali tedesche all'estero non si limita a un obbligo legale puramente oggettivo (applicabile Hölscheidt, Jura 2017, p. 148 <150 f.>; aA Löffelmann, in: Dietrich / Gärditz / Graulich / Gusy / Warg [Ed.], Riforma dei servizi di intelligence tra legalizzazione e internazionalizzazione, 2019, p. 33 <38>). Piuttosto, corrisponde a

un diritto fondamentale di coloro che sono identificati come diritti fondamentali protetti dalle rispettive garanzie sui diritti fondamentali. La Legge fondamentale non prevede un vincolo dei diritti fondamentali a favore dei singoli titolari dei diritti fondamentali, che tuttavia non è contrastato da alcun equivalente giuridico soggettivo. Il carattere come diritto individuale appartiene al contenuto centrale della protezione dei diritti fondamentali.

93

2. Il vincolo dei diritti fondamentali da parte delle autorità tedesche, anche quando si tratta di stranieri all'estero, corrisponde anche all'integrazione della Repubblica federale nella comunità internazionale.

94

a) All'articolo 1, paragrafo 2, della Legge fondamentale, la Legge fondamentale riconosce i diritti umani inviolabili e inalienabili come base di ogni comunità umana, pace e giustizia nel mondo. I diritti fondamentali della Legge fondamentale sono quindi collocati nel contesto delle garanzie internazionali sui diritti umani che mirano alla protezione oltre i confini nazionali che si applica alle persone come persone. Di conseguenza, l'articolo 1, paragrafo 2 e l'articolo 1, paragrafo 3 della Legge fondamentale si collegano alla garanzia della dignità umana dell'articolo 1, paragrafo 1 della Legge fondamentale. In connessione con questa integrazione universalistica della protezione dei diritti fondamentali, la Legge fondamentale fa deliberatamente una distinzione tra diritti tedeschi e diritti umani per la strutturazione legale positiva dei diritti fondamentali. Ma questo non suggerisceanche per limitare i diritti umani alle questioni interne o per agire a livello nazionale. Tale comprensione non si trova nella formulazione della Legge fondamentale. In particolare, tale limitazione non deriva dal preambolo della Legge fondamentale, che, con riferimento al "popolo tedesco nei paesi", non è territoriale, ma è formulata dal punto di vista degli attori costituenti e della responsabilità del popolo tedesco in un'Europa unita e Welt sottolinea (cfr. Jarass, in: Jarass / Pieroth, GG, 15a edizione 2018, preambolo paragrafo 9, art. 1 Rn. 44; Kahl, in: commento Bonner, GG, art. 1 Abs. 3 Rn. 199 f. [2014]; Murswiek, in: Bonner Kommentar, GG, preambolo nm. 306 [2005]; aA Löffelmann, in: Dietrich / Eiffler [ed.], Handbuch des Nachrichtendienstes, 2017, VI § 3 nm. 15).

95

La distinzione terminologica tra "diritti umani inviolabili e inalienabili" secondo l'articolo 1 capoverso 2 GG e i "diritti fondamentali successivi" di cui all'articolo 1 capoverso 3 GG non si oppone all'integrazione dei diritti fondamentali nel contesto dei diritti umani universalmente applicabili. Anche a questo proposito, la formulazione e la sistematica della Legge fondamentale non mostrano alcuna interpretazione relativa alla distinzione nel senso di aree di applicazione spaziale separate. Il fatto che i diritti fondamentali della Legge fondamentale (Art. 1 Paragrafo 3 GG) siano al contrario legati alla garanzia dei diritti umani è dimostrato anche dalla costante giurisprudenza della Corte costituzionale federale, secondo la quale i diritti fondamentali della Legge fondamentale devono essere interpretati alla luce delle garanzie internazionali sui diritti umani (vedi BVerfGE 111 , 307 <317 f.>; 128, 282 <306 f.>; 128, 326 <367 f.>; 142, 313 <345 marg. 88>; 148, 296 <351 marg. 128>; BVerfG, decisione del Primo Senato del 6 novembre 2019 - 1 BvR 16/13 -, marg. 58 - Diritto all'oblio I). I principi di cui all'articolo 1, paragrafo 2, GG ai sensi dell'articolo 79, paragrafo 3, GG costituiscono un limite assoluto per le restrizioni alla protezione dei diritti fondamentali da parte del legislatore costituzionale (vedi BVerfGE 84, 90 <120 f.>; 141, 1 <15 paragrafo 34>).3 GG un limite assoluto per le restrizioni alla protezione dei diritti fondamentali da parte del legislatore costituzionale (cfr. BVerfGE 84, 90 <120 f.>; 141, 1 <15 para.

34>).3 GG un limite assoluto per le restrizioni alla protezione dei diritti fondamentali da parte del legislatore costituzionale (cfr. BVerfGE 84, 90 <120 f.>; 141, 1 <15 para. 34>).

96

Questo legame tra i diritti fondamentali e la garanzia dei diritti umani non sarebbe compatibile con una comprensione dei diritti fondamentali della Legge fondamentale, il che significa che la loro validità termina ai confini dello stato e libera le autorità tedesche nei confronti degli stranieri dai loro obblighi in materia di diritti umani e fondamentali all'estero. Ciò minerebbe l'affermazione della Legge fondamentale, basata su convenzioni internazionali in cooperazione oltre i confini nazionali, dei diritti inalienabili di ogni persona - compresa la protezione contro la sorveglianza (cfr. Art. 12 AEMR; art. 17 cpv. 1 IPbpR). Date le condizioni dell'internazionalizzazione delle condizioni politiche di azione e un crescente impegno degli Stati oltre i propri confini, ciò dovrebbe portare ache la protezione dei diritti fondamentali della Legge fondamentale non segue un raggio d'azione allargato dell'autorità statale tedesca e - al contrario - potrebbe persino essere compromessa dalla cooperazione degli Stati. Al contrario, il collegamento dei diritti fondamentali con lo stato come soggetto politicamente legittimo e legato all'azione garantisce che la protezione dei diritti fondamentali segua anche un'espansione internazionale delle attività statali.che la protezione dei diritti fondamentali segue anche un'espansione internazionale delle attività statali.che la protezione dei diritti fondamentali segue anche un'espansione internazionale delle attività statali.

97

b) Una simile comprensione della portata dei diritti fondamentali della Legge fondamentale è suggerita anche dalla Convenzione europea dei diritti dell'uomo, che dovrebbe essere utilizzata come aiuto per l'interpretazione nell'interpretazione dei diritti fondamentali (vedi BVerfG, decisione del Primo Senato del 6 novembre 2019 - 1 BvR 16/13 - 58 mwN - diritto all'oblio I). La misura in cui le loro garanzie si applicano alle azioni degli Stati della Convenzione al di fuori del loro territorio non è ancora completa chiarito. La Corte europea dei diritti dell'uomo si basa sul criterio di un controllo effettivo sull'azione sul territorio straniero e in molti casi ha riconosciuto la validità internazionale dei diritti della convenzione su questa base (cfr. In sintesi EGMR [GK], Al -Skeini e altri c. Regno Unito, sentenza del 7 luglio 2011, n. 55721/07, §§ 132 ss. MwN; vedere anche Aust, AVR 52 <2014>, p. 375 <394 ss.> MwN) . Tuttavia, non vi è alcun chiarimento finale vincolante sulla questione della protezione contro le misure di sorveglianza da parte degli Stati della Convenzione in altri Stati .

98

Tuttavia, la 1a Sezione della Corte europea dei diritti dell'uomo ha misurato senza riserve l'attuazione delle misure di sorveglianza con obiettivi all'estero in una decisione che non è ancora giuridicamente vincolante e l'ha trovata contraria alla convenzione, in base alla quale i denuncianti includevano cittadini stranieri che non erano nello stato della convenzione o vissuto lì (vedi EGMR, Big Brother Watch e altri c. Regno Unito, sentenza del 13 settembre 2018, n. 58170/13 e altri, § 271). Allo stesso modo, i poteri di supervisione strategica di diritto svedese, che erano stati attaccati da un'organizzazione non governativa svedese e che avevano escluso la comunicazione interna, sono stati controllati contro la convenzione senza mettere in discussione la validità internazionale (cfr. CEDU,Centro per Rättvisa v. Svezia, sentenza del 19 giugno 2018, n. 35252/08). Entrambi i casi sono attualmente pendenti dinanzi alla Grande Camera.

99

Indipendentemente dall'esito di questi procedimenti, la Convenzione europea sui diritti umani non ostacola la validità internazionale dei diritti fondamentali tedeschi. Perché, in quanto contratto di diritto internazionale, ha una portata definita indipendentemente dalla quale non possono derivare derivazioni dirette in alcun caso per la portata della protezione dei diritti fondamentali ai sensi della Legge fondamentale. In ogni caso, non esclude l'ulteriore tutela dei diritti fondamentali da parte degli Stati della Convenzione (art. 53 CEDU).

100

c) Il vincolo dei diritti fondamentali da parte delle potenze statali tedesche all'estero non è in conflitto con il fatto che sarebbe necessaria una differenziazione o un coordinamento con altri stati e ordinanze giuridiche, poiché la Corte costituzionale federale considera - l'unica - possibile ragione per escludere l'obbligo dall'Art 10 GG aveva preso in considerazione e lasciato aperto in caso di questioni estere (vedi BVerfGE 100, 313 <362 e seguenti>).

101

Il vincolo ai diritti fondamentali tedeschi crea solo una responsabilità e responsabilità degli organi statali tedeschi. Accompagna da solo le decisioni politiche autonome della Repubblica federale di Germania e limita solo il proprio campo d'azione. Di conseguenza, i diritti fondamentali come diritti di difesa funzionano anche all'estero solo contro l'autorità statale tedesca e quindi vanno di pari passo con le restrizioni basate sul divieto di intervento del diritto internazionale. Il vincolo dei diritti fondamentali non costituisce pertanto una violazione del diritto internazionale che vieta l'intervento, né limita il potere di agire o legiferare in altri paesi. Non ha effetto su un Oktroi secondo la propria legge né sopprime i diritti fondamentali stranieri. In particolare, il vincolo dei diritti fondamentali estende i poteri non statali all'estero,ma limita solo il potenziale di intervento delle autorità statali tedesche.

102

Di conseguenza, la validità dei diritti fondamentali (qui articolo 10.1 GG) non influisce sull'ordinamento giuridico di altri paesi e i poteri di intervento associati per le misure di sorveglianza per il loro ordinamento giuridico interno non hanno alcun effetto normativo. Dalla validità dei diritti fondamentali e dalla riserva legale segue solo che le basi giuridiche corrispondenti devono essere create per le autorità tedesche, a condizione che le misure di sorveglianza debbano essere applicate anche agli stranieri all'estero. Non specifica se e in quale misura tali poteri siano effettivamente creati e utilizzati. A questo proposito, non si dice nulla sulla giustificazione di singole misure basate su tali poteri per quanto riguarda il loro impatto esterno sul rispettivo paese di destinazione.

103

Dal vincolo dei diritti fondamentali in quanto tali, non sussiste nulla per la questione se tali misure siano ammissibili ai sensi del diritto internazionale. Inoltre, agli altri Stati non viene impedito di difendersi contro tali misure nella propria area - così come ciò può essere richiesto anche dalla legge costituzionale tedesca contro le misure di sorveglianza da parte di servizi stranieri a livello nazionale (sotto il margine n. 249). A questo proposito, il vincolo dell'autorità statale tedesca ai diritti fondamentali non grava su altri stati che potrebbero sollevare preoccupazioni ai sensi del diritto internazionale (cfr. Baker, KuR 2014, p. 556 <561>; Becker, NVwZ 2015, p. 1335 <1339>; Gärditz, L'amministrazione 48 <2015>, p. 463 <472 f.>). Di conseguenza, non è raro a livello internazionale creare basi legali per misure di sorveglianza che si applicano anche agli stranieri

all'estero.Solo loro hanno una funzione di autorizzazione interna (vedi Gusy, in: Schenke / Graulich / Ruthig [ed.], Federal Security Law, 2nd edition 2019, § 1 BNDG Rn. 56; ad es. Per gli Stati Uniti: Sezione 702 Foreign Intelligence Surveillance Act; vedi Renan, in: Goldman / Rascoff [ed.], Global Intelligence Oversight, 2016, p. 121 <123 ss.>; Per il Regno Unito fino al 2017: Sezione 8 [4] Regulation of Investigatory Powers Act; per il Regno Unito dal 2017: Parte 6 Capitolo 1 Investigatory Powers Act 2016; vedi Leigh, in: Dietrich / Sule [ed.], Intelligence Law and Policies in Europe, 2019, p. 553 e seguenti; McKay / Walker, in: Dietrich / Gärditz / Graulich / Gusy / Warg [ed.], Riforma dei servizi di intelligence tra legalizzazione e internazionalizzazione, 2019, p. 119 e seguenti; per la Francia:Articoli da L854-1 a L854-9 Codice della sicurezza interna [Messaggi di sorveglianza delle comunicazioni elettroniche internazionali]; vedere. Le Divelec, in: Dietrich / Sule [ed.], Legge e politiche sull'intelligence in Europa, 2019, 516 e seguenti; Warusfel, in: Dietrich / Gärditz / Graulich / Gusy / Warg [ed.], Riforma dei servizi di intelligence tra legalizzazione e internazionalizzazione, 2019, p. 129 ss.).

104

3. Il collegamento globale dell'autorità statale tedesca con i diritti fondamentali non influisce sul fatto che gli effetti protettivi derivanti dai diritti fondamentali possono differire a seconda delle circostanze in cui sono utilizzati. Ciò vale - come già accade per le diverse dimensioni dell'efficacia dei diritti fondamentali in Germania - alla portata del loro effetto protettivo all'estero. Ad esempio, le garanzie individuali in Germania e all'estero possono richiedere diversi gradi in relazione all'area di protezione personale e materiale (sotto, nm. 196). È inoltre possibile operare una distinzione tra le diverse dimensioni dei diritti fondamentali, come l'effetto dei diritti fondamentali come diritti della difesa, diritti delle prestazioni, decisioni costituzionali sul valore o base degli obblighi di protezione.Nella misura in cui i diritti fondamentali dipendono dalle specifiche del legislatore, potrebbero essere prese in considerazione anche le condizioni speciali all'estero (vedere BVerfGE 92, 26 <41 ss.>; Anche BVerfGE 100, 313 <363>). L'integrazione dell'azione del governo in un ambiente straniero deve essere presa in considerazione quando si determinano i requisiti per la giustificazione delle violazioni dei diritti fondamentali, in particolare nel contesto della proporzionalità.L'integrazione dell'azione del governo in un ambiente straniero deve essere presa in considerazione quando si determinano i requisiti per la giustificazione delle violazioni dei diritti fondamentali, in particolare nel contesto della proporzionalità.L'integrazione dell'azione del governo in un ambiente straniero deve essere presa in considerazione quando si determinano i requisiti per la giustificazione delle violazioni dei diritti fondamentali, in particolare nel contesto della proporzionalità.

105

4. Si tratta della protezione contro le misure di sorveglianza nel contesto della ricognizione delle telecomunicazioni estere da parte dei diritti fondamentali di cui all'articolo 10 capoverso 1 e all'articolo 5 capoverso. Come risulta dalle spiegazioni di cui sopra, i diritti fondamentali vincolanti fondamentali delle autorità tedesche, in ogni caso, vincolano anche il Servizio di intelligence federale e il legislatore a disciplinarne i poteri. La Legge fondamentale non sa tanto dell'esenzione delle misure di raccolta di informazioni dal vincolo dei diritti fondamentali a causa del loro orientamento estero quanto del loro carattere politico. Piuttosto, il vincolo globale dei diritti fondamentali di cui all'articolo 1, paragrafo 3, GG crea le condizioni peressere in grado di tener conto delle minacce ai diritti fondamentali derivanti da nuovi sviluppi tecnici e dal conseguente spostamento delle forze. Ciò vale in particolare per la mutevole importanza dei servizi di intelligence nel corso dell'ulteriore sviluppo della tecnologia dell'informazione e del conseguente accesso all'estero.

106

a) L'intelligence all'estero è sempre stata di notevole importanza per la capacità della Repubblica federale di Germania di agire nell'ambito della politica estera e di sicurezza, ma recentemente ha acquisito importanza. Nel corso dello sviluppo della tecnologia dell'informazione e dell'internazionalizzazione, l'importanza e le condizioni dell'intelligence delle telecomunicazioni all'estero sono cambiate sostanzialmente come elemento centrale dell'intelligence dell'intelligence all'estero.

107

In passato, l'educazione alle telecomunicazioni mirava esclusivamente alla diagnosi precoce del pericolo al fine di evitare attacchi armati sul territorio federale e le misure personali erano limitate a un piccolo gruppo di persone, sia in termini di tecnologia che di conoscenze (cfr. VerfGE 67, 157 <178>). Nel corso delle odierne opzioni di comunicazione e del contesto d'azione internazionalizzato associato, i potenziali pericoli provenienti dall'estero si sono moltiplicati. La tecnologia dell'informazione consente di comunicare tra loro direttamente e senza ostacoli attraverso le distanze spaziali e di coordinarsi senza perdere tempo. Ciò crea nuove sfide per l'acquisizione di comunicazioni politicamente o militarmente rilevanti,che può essere di notevole importanza per la capacità di azione del governo federale. Le attività internazionali possono anche avere un effetto destabilizzante sull'intera comunità, come si può vedere, ad esempio, in attacchi informatici, criminalità organizzata a livello internazionale come traffico di esseri umani o riciclaggio di denaro e terrorismo internazionale (vedi Kojm, in: Goldman / Rascoff [ed.], Global Intelligence Oversight, 2016, pagg. 95 e seguenti; Goodman / Ischebeck-Baum, in: Dietrich / Sule [ed.], Intelligence Law and Policies in Europe, 2019, p. 1 <marginal 104 ff.>; Rosand, Journal of Conflict & Legge sulla sicurezza 11 <2006>, p. 399 <400 f.>; Per quanto riguarda la zona di pericolo "Cyber", vedere anche BTDrucks 18/4654, p. 40 f.).L'intelligence straniera mediante la sorveglianza delle telecomunicazioni sta pertanto diventando sempre più importante in termini di politica estera e di sicurezza, che si riflette anche politicamente, ad esempio, nei bilanci di bilancio dei servizi di intelligence, che sono aumentati in modo significativo rispetto a molte altre aree (cfr. Raddoppiare il bilancio stimato del Servizio federale di intelligence di 475,5 milioni Euro nel 2011 [cfr. Conti del bilancio federale per il 2011, p. 185] a 966,5 milioni di euro nel 2019 [cfr. Budget Act 2019 del 17 dicembre 2018, BGBl I p. 2528, sezione 04, p. 22], mentre nello stesso periodo il bilancio totale da 306,8 miliardi di euro [cfr. Bilancio federale per il 2011, p. 14] a 356,4 miliardi di euro [cfr. Legge sul bilancio 2019 del 17 dicembre 2018, BGBl I S 2528, piano generale, p.16] è aumentato del 16 percento).

108

b) La crescente importanza dell'intelligence straniera nel mutare delle condizioni nello spazio di tensione tra libertà e sicurezza va di pari passo con le nuove sfide non solo per salvaguardare la sicurezza, ma anche per salvaguardare la libertà, che deve essere bilanciata conformemente allo stato di diritto sulla base dei diritti fondamentali.

109

Gli sviluppi nella tecnologia dell'informazione sono associati al fatto che i flussi di dati tramite satelliti e cavi sono condotti in modo volatile in tutto il mondo secondo criteri tecnici indipendenti dai confini nazionali (cfr. BTDrucks 14/5655, p. 17 per questo sviluppo). Ciò consente di registrare comunicazioni estere in misura considerevole, anche dall'interno della Germania. Allo stesso tempo, la comunicazione sociale si svolge sempre più in un contesto internazionale. Sulla base dei

servizi transfrontalieri, lo scambio tra cittadini è sostenuto come detentore di diritti fondamentali, sia all'interno che tra gli Stati - in gran parte sui servizi di telecomunicazione che non sono strutturati in base alla distinzione tra domestico e straniero (vedi Kojm, in: Goldman / Rascoff [ed.], Global Intelligence Oversight, 2016, p. 95 <100 f.>). Sullo sfondo del fatto che nelle attuali condizioni della tecnologia dell'informazione, le azioni e le relazioni di comunicazione di ogni tipo si riflettono sempre più in forma digitale e in vista delle capacità di elaborazione dei dati in costante aumento, le possibilità di sorveglianza delle telecomunicazioni si estendono a vaste aree dell'intera società civile, anche al di fuori del proprio territorio - e viceversa La comunicazione interna è anche soggetta alla sorveglianza di altri paesi (vedi BTDrucks 18/12850, p. 1283 ss.).

110

La comprensione dei diritti fondamentali, che porrebbe fine alla loro validità ai confini dello stato, lascia i diritti fondamentali indifesi di fronte a tali sviluppi e farebbe rientrare la portata della protezione dei diritti fondamentali dietro le condizioni dell'internazionalizzazione (vedi Becker, NVwZ 2015, p. 1335 <1339>; paper, NVwZ 2017, p. 3025 <3029>; Marxsen, DÖV 2018, p. 218 <226>). Potrebbe portare al La protezione dei diritti fondamentali in un'area sempre più importante di azione statale ad alta intensità di intervento e - con la legge sulla sicurezza - in un'area in cui i diritti fondamentali sono in genere di particolare importanza sarebbe vuota. Collegando Art. 1 Paragrafo 3 GG allo stato come soggetto, tiene anche conto di tali nuove potenziali minacce e aiuta a classificarle nel quadro costituzionale generale della Legge fondamentale.

II.

111

1. Le disposizioni impugnate riguardano i denuncianti nei loro diritti fondamentali di cui all'articolo 10 capoverso 1 e all'articolo 5 capoverso 1 frase 2 GG. Autorizzano la raccolta di dati personali mediante sorveglianza segreta delle telecomunicazioni e incidono quindi sul contenuto di garanzia del segreto sulle telecomunicazioni protetto dall'articolo 10.1 della Legge fondamentale. In relazione a ciò, la trasmissione dei dati ottenuti da tali misure incide anche sulla protezione del segreto delle telecomunicazioni, cosicché anche questi possono essere misurati in base all'articolo 10 GG. Le disposizioni contestate riguardano anche i denuncianti che lavorano come giornalisti nel loro diritto fondamentale ai sensi dell'articolo 5, paragrafo 1, frase 2 GG. Perché autorizzano il servizio di intelligence federale a raccogliereElaborazione e trasmissione di dati dalle telecomunicazioni nel contesto della loro attività professionale, compreso il monitoraggio mirato e la valutazione della loro comunicazione in questo contesto, ad esempio con informatori (cfr. EGMR, Weber e Saravia c. Germania, decisione del 29 giugno 2006, n. 54934 / 00, §§ 143 e seguenti; Big Brother Watch e altri contro Regno Unito, sentenza del 13 settembre 2018, n. 58170/13 e altri, §§ 476, 490 e seguenti; vedere anche BVerfGE 100, 313 <365>) .vedi anche BVerfGE 100, 313 <365>).vedi anche BVerfGE 100, 313 <365>).

112

2. Nel presente procedimento non è necessario chiarire se i regolamenti impugnati siano compatibili con i requisiti di uguaglianza per quanto riguarda la distinzione tra tedeschi e cittadini dell'Unione. A questo proposito, deve rimanere aperto in particolare se la Sezione 6 (3) BNDG, anche in combinato disposto con la Sezione 14 (2) BNDG, crea una differenziazione giustificata dal punto di vista fattuale a tale riguardo. Perché la questione della parità di trattamento dei cittadini tedeschi e dei cittadini dell'Unione non solo trova gli standard nella Legge fondamentale, ma solleva anche questioni irrisolte del diritto dell'Unione; ciò include già la sua applicabilità in vista dell'articolo 4

paragrafo 2 del TUE e delle libertà fondamentali e quindi, se del caso, l'ambito di applicazione del divieto di discriminazione ai sensi del diritto dell'UE (vedi Kreuter / Möbius, BWV 2009, p. 146 <148>; Hölscheidt, Jura 2017, P. 148 <156>;Marxsen, DÖV 2018, p. 218 <224>; vedere. anche i procedimenti pendenti dinanzi alla CGUE, Privacy International, C-623/17, GU UE 2018 / C 022/41 [Regno Unito]; La Quadrature du Net e altri, C-511/18, GU UE 2018 / C 392/10 e Rete dati francese e altri, C-512/18, GU UE 2018 / C 392/11 [ogni Francia]). La Corte costituzionale federale non può da sola chiarire la questione di quali requisiti di uguaglianza sono soggetti al legislatore nel progettare il monitoraggio strategico. Non può sottoporre questa questione alla Corte di giustizia europea a causa della mancanza di potere decisionale, poiché le disposizioni controverse sono incostituzionali per soli motivi formali (margine n. 134 e seguenti). In queste circostanze, non vi sono ulteriori chiarimenti materiali su queste domande in base alla Legge fondamentale.DÖV 2018, p. 218 <224>; vedere. anche i procedimenti pendenti dinanzi alla CGUE, Privacy International, C-623/17, GU UE 2018 / C 022/41 [Regno Unito]; La Quadrature du Net e altri, C-511/18, GU UE 2018 / C 392/10 e Rete dati francese e altri, C-512/18, GU UE 2018 / C 392/11 [ogni Francia]). La Corte costituzionale federale non può da sola chiarire la questione di quali requisiti di uguaglianza sono soggetti al legislatore nel progettare il monitoraggio strategico. Non può sottoporre questa questione alla Corte di giustizia europea a causa della mancanza di potere decisionale, poiché le disposizioni controverse sono incostituzionali per soli motivi formali (margine n. 134 e seguenti). In queste circostanze, non vi sono ulteriori chiarimenti materiali su queste domande in base alla Legge fondamentale.DÖV 2018, p. 218 <224>; vedere. anche i procedimenti pendenti dinanzi alla CGUE, Privacy International, C-623/17, GU UE 2018 / C 022/41 [Regno Unito]; La Quadrature du Net e altri, C-511/18, GU UE 2018 / C 392/10 e Rete dati francese e altri, C-512/18, GU UE 2018 / C 392/11 [ogni Francia]). La Corte costituzionale federale non può da sola chiarire la questione di quali requisiti di uguaglianza sono soggetti al legislatore nel progettare il monitoraggio strategico. Non può sottoporre questa questione alla Corte di giustizia europea a causa della mancanza di potere decisionale, poiché le disposizioni controverse sono incostituzionali per soli motivi formali (margine n. 134 e seguenti). In queste circostanze, non vi sono ulteriori chiarimenti materiali su queste domande in base alla Legge fondamentale.218 <224>; vedere. anche i procedimenti pendenti dinanzi alla CGUE, Privacy International, C-623/17, GU UE 2018 / C 022/41 [Regno Unito]; La Quadrature du Net e altri, C-511/18, GU UE 2018 / C 392/10 e Rete dati francese e altri, C-512/18, GU UE 2018 / C 392/11 [ogni Francia]). La Corte costituzionale federale non può da sola chiarire la questione di quali requisiti di uguaglianza sono soggetti al legislatore nel progettare il monitoraggio strategico. Non può sottoporre questa questione alla Corte di giustizia europea a causa della mancanza di potere decisionale, poiché le disposizioni controverse sono incostituzionali per soli motivi formali (margine n. 134 e seguenti). In queste circostanze, non vi sono ulteriori chiarimenti materiali su queste domande in base alla Legge fondamentale.218 <224>; vedere. anche i procedimenti pendenti dinanzi alla CGUE, Privacy International, C-623/17, GU UE 2018 / C 022/41 [Regno Unito]; La Quadrature du Net e altri, C-511/18, GU UE 2018 / C 392/10 e Rete dati francese e altri, C-512/18, GU UE 2018 / C 392/11 [ogni Francia]). La Corte costituzionale federale non può da sola chiarire la questione di quali requisiti di uguaglianza sono soggetti al legislatore nel progettare il monitoraggio strategico. Non può sottoporre questa questione alla Corte di giustizia europea a causa della mancanza di potere decisionale, poiché le disposizioni controverse sono incostituzionali per soli motivi formali (margine n. 134 e seguenti). In queste circostanze, non vi sono ulteriori chiarimenti materiali su queste domande in base alla Legge fondamentale.anche i procedimenti pendenti dinanzi alla CGUE, Privacy International, C-623/17, GU UE 2018 / C 022/41 [Regno Unito]; La Quadrature du Net e altri, C-511/18, GU UE 2018 / C 392/10 e Rete dati francese e altri, C-512/18, GU UE 2018 / C 392/11 [ogni Francia]). La Corte costituzionale federale non può da sola chiarire la questione di quali requisiti di uguaglianza sono soggetti al legislatore nel progettare il monitoraggio strategico. Non può sottoporre questa questione alla Corte di giustizia europea a causa della mancanza di potere decisionale, poiché le disposizioni controverse sono incostituzionali per soli motivi formali (margine n. 134 e seguenti). In queste circostanze, non vi

sono ulteriori chiarimenti materiali su queste domande in base alla Legge fondamentale.anche i procedimenti pendenti dinanzi alla CGUE, Privacy International, C-623/17, GU UE 2018 / C 022/41 [Regno Unito]; La Quadrature du Net e altri, C-511/18, GU UE 2018 / C 392/10 e Rete dati francese e altri, C-512/18, GU UE 2018 / C 392/11 [ogni Francia]). La Corte costituzionale federale non può da sola chiarire la questione di quali requisiti di uguaglianza sono soggetti al legislatore nel progettare il monitoraggio strategico. Non può sottoporre questa questione alla Corte di giustizia europea a causa della mancanza di potere decisionale, poiché le disposizioni controverse sono incostituzionali per soli motivi formali (margine n. 134 e seguenti). In queste circostanze, non vi sono ulteriori chiarimenti materiali su queste domande in base alla Legge fondamentale.Privacy International, C-623/17, OJEU 2018 / C 022/41 [Regno Unito]; La Quadrature du Net e altri, C-511/18, GU UE 2018 / C 392/10 e Rete dati francese e altri, C-512/18, GU UE 2018 / C 392/11 [ogni Francia]). La Corte costituzionale federale non può da sola chiarire la questione di quali requisiti di uguaglianza sono soggetti al legislatore nel progettare il monitoraggio strategico. Non può sottoporre questa questione alla Corte di giustizia europea a causa della mancanza di potere decisionale, poiché le disposizioni controverse sono incostituzionali per soli motivi formali (margine n. 134 e seguenti). In queste circostanze, non vi sono ulteriori chiarimenti materiali su queste domande in base alla Legge fondamentale.Privacy International, C-623/17, OJEU 2018 / C 022/41 [Regno Unito]; La Quadrature du Net e altri, C-511/18, GU UE 2018 / C 392/10 e Rete dati francese e altri, C-512/18, GU UE 2018 / C 392/11 [ogni Francia]). La Corte costituzionale federale non può da sola chiarire la questione di quali requisiti di uguaglianza sono soggetti al legislatore nel progettare il monitoraggio strategico. Non può sottoporre questa questione alla Corte di giustizia europea a causa della mancanza di potere decisionale, poiché le disposizioni controverse sono incostituzionali per soli motivi formali (margine n. 134 e seguenti). In queste circostanze, non vi sono ulteriori chiarimenti materiali su queste domande in base alla Legge fondamentale.La Quadrature du Net e altri, C-511/18, GU UE 2018 / C 392/10 e Rete dati francese e altri, C-512/18, GU UE 2018 / C 392/11 [ogni Francia]). La Corte costituzionale federale non può da sola chiarire la questione di quali requisiti di uguaglianza sono soggetti al legislatore nel progettare il monitoraggio strategico. Non può sottoporre questa questione alla Corte di giustizia europea a causa della mancanza di potere decisionale, poiché le disposizioni controverse sono incostituzionali per soli motivi formali (margine n. 134 e seguenti). In queste circostanze, non vi sono ulteriori chiarimenti materiali su queste domande in base alla Legge fondamentale.La Quadrature du Net e altri, C-511/18, GU UE 2018 / C 392/10 e Rete dati francese e altri, C-512/18, GU UE 2018 / C 392/11 [ogni Francia]). La Corte costituzionale federale non può da sola chiarire la questione di quali requisiti di uguaglianza sono soggetti al legislatore nel progettare il monitoraggio strategico. Non può sottoporre questa questione alla Corte di giustizia europea a causa della mancanza di potere decisionale, poiché le disposizioni controverse sono incostituzionali per soli motivi formali (margine n. 134 e seguenti). In queste circostanze, non vi sono ulteriori chiarimenti materiali su queste domande in base alla Legge fondamentale.La sola Corte costituzionale federale non è in grado di determinare a quali requisiti di uguaglianza è soggetta la legislatura nel progettare il monitoraggio strategico. Non può sottoporre questa questione alla Corte di giustizia europea a causa della mancanza di potere decisionale, poiché le disposizioni controverse sono incostituzionali per soli motivi formali (margine n. 134 e seguenti). In queste circostanze, non vi sono ulteriori chiarimenti materiali su queste domande in base alla Legge fondamentale.La sola Corte costituzionale federale non è in grado di determinare a quali requisiti di uguaglianza è soggetta la legislatura nel progettare il monitoraggio strategico. Non può sottoporre questa questione alla Corte di giustizia europea a causa della mancanza di potere decisionale, poiché le disposizioni controverse sono incostituzionali per soli motivi formali (margine n. 134 e seguenti). In queste circostanze, non vi sono ulteriori chiarimenti materiali su queste domande in base alla Legge fondamentale.poiché le disposizioni controverse sono incostituzionali per motivi formali (margine 134 f. sotto). In queste circostanze, non vi sono ulteriori chiarimenti materiali su queste domande in base alla Legge fondamentale.poiché le disposizioni controverse sono incostituzionali per motivi formali (margine

134 f. sotto). In queste circostanze, non vi sono ulteriori chiarimenti materiali su queste domande in base alla Legge fondamentale.

III.

113

I regolamenti impugnati giustificano l'interferenza con i diritti fondamentali a vari livelli.

114

1. L'art. 6, n. 1, del BNDG autorizza inizialmente il Servizio di intelligence federale a registrare il traffico di telecomunicazioni individuale dalle reti specificate per ordine; Ciò apre in particolare l'intercettazione dei segnali satellitari e l'acquisizione di flussi di dati collegati alla linea, sia per mezzo dei nostri dispositivi sia per mezzo di una deviazione organizzata conformemente alla Sezione 8 BNDG. Di conseguenza, la Sezione 14 (1) BNDG autorizza il Servizio di intelligence federale a raccogliere dati personali nel contesto della cooperazione con i servizi di intelligence stranieri.

115

a) In relazione ai denuncianti da 1) a 7) come cittadini stranieri che vivono all'estero, questo tipo di registrazione comporta un intervento. Una tale raccolta di dati personali in senso costituzionale è una raccolta di dati. Rende i dati delle persone colpite specificamente accessibili al Servizio di intelligence federale in modo da poterli valutare in base a criteri di contenuto - sia sulla base di termini di ricerca per l'immissione di dati di contenuto, sia per la valutazione (eventualmente accumulando) dati sul traffico o per la trasmissione a quelli stranieri enti pubblici nell'ambito di una cooperazione. I dati che verranno successivamente respinti non saranno solo registrati involontariamente, ma anche raccolti consapevolmente,al fine di essere valutato per i risultati pertinenti e, se necessario, da utilizzare (vedere anche BVerfGE 100, 313 <366>).

116

b) Alla luce dell'attuale stato dell'arte, ciò vale anche per il denunciante di 8), che è cittadino tedesco. Poiché la Sezione 6 (4) BNDG (possibilmente in combinato disposto con la Sezione 14 (2) BNDG) non consente misure di sorveglianza contro cittadini e residenti tedeschi, non vi è praticamente alcun intervento nella registrazione iniziale dei dati. Questi dati vengono registrati solo in modo non mirato e unicamente per motivi tecnici e devono essere riordinati immediatamente dopo l'elaborazione del segnale utilizzando vari processi di filtraggio senza lasciare tracce tecniche. L'interesse ufficiale per i dati raccolti non è aumentato a tal punto che si può presumere che abbia una qualità che innesca una violazione dei diritti fondamentali (vedere BVerfGE 100, 313 <366>; 115, 320 <343>;150, 244 <266 marg. 43>).

117

Tuttavia, secondo lo stato dell'arte attuale, non è possibile filtrare completamente i dati di cittadini e residenti tedeschi, in modo che anche alcuni di questi dati vengano valutati. Vengono quindi risolti solo quando vengono identificati a mano. La sezione 6 (1) e (4) BNDG non lo consente in modo chiaramente riconoscibile, ma richiede tale comprensione per essere applicabile; è così che il regolamento è sempre stato compreso nella pratica. Ciò costituisce un intervento in relazione a persone i cui dati vengono registrati in questo modo senza essere tecnicamente separati dopo

l'elaborazione del segnale e che vengono così presi in considerazione dai dipendenti del Servizio federale di informazione. Con § 6 capoverso 1, comma4 BNDG fornisce la base giuridica per questo, dà anche diritto al denunciante a 8) di intervenire nel suo diritto fondamentale ai sensi dell'articolo 10.1 della Legge fondamentale.

118

2. La sezione 6, paragrafi da 1 a 3, BNDG giustifica ulteriori interventi sui diritti fondamentali nei confronti dei denuncianti, autorizzandoli a valutare ulteriormente i dati. Da un lato, la sezione 6 (1) BNDG e, nella misura ivi regolamentata, la sezione 14 (1) BNDG in combinato disposto con la sezione 19 (1) BNDG autorizzano un intervento sotto forma di valutazione dei dati sul traffico delle telecomunicazioni raccolti, che possono anche essere memorizzati. D'altra parte, § 6 paragrafi da 1 a 3 BNDG autorizza la valutazione della telecomunicazione registrata usando termini di ricerca per visualizzare i dati del contenuto. Ulteriori interventi risiedono nella valutazione manuale del traffico di telecomunicazioni filtrato, che è ugualmente coperto dal regolamento,che comprende l'ulteriore elaborazione dei dati - dalla visualizzazione del traffico delle telecomunicazioni assorbito mediante termini di ricerca, attraverso la loro decodifica e segnalazione alle cosiddette "aree decrescenti", fino al loro utilizzo lì.

119

3. La propria interferenza con i diritti fondamentali risiede nella possibile trasmissione delle conoscenze risultanti dal monitoraggio, nella misura in cui contenga dati personali, come previsto dal § 24 BNDG in vari casi individuali. I dati ottenuti sono resi disponibili ad altre autorità, il che significa sempre un'intrusione di diritti fondamentali (vedi BVerfGE 141, 220 <324 f. Margine n. 279>). Di conseguenza, la trasmissione automatizzata di informazioni a enti pubblici stranieri, come previsto dalla Sezione 15 (1) BNDG nel contesto della cooperazione, comporta un'interferenza con i diritti fondamentali.

120

4. Interventi nell'articolo 10 capoverso 1 GG e, se applicabile, nell'articolo 5 capoverso 1 frase 2 GG giustifica anche § 7 BNDG. Sebbene ciò non regoli direttamente la raccolta di dati attraverso le misure di sorveglianza stessa, la presuppone (cfr. Dietrich, in: Schenke / Graulich / Ruthig [ed.], Sicherheitrechts des Bundes, 2a edizione 2019, § 7 BNDG Rn. 2 ; Marxsen, DÖV 2018, p. 218 <223>; Löffelmann, in: Dietrich / Gärditz / Graulich / Gusy / Warg [ed.], Riforma dei servizi di intelligence tra legalizzazione e internazionalizzazione, 2019, p. 33 <39>). La sezione 7 (1) BNDG, tuttavia, giustifica l'ulteriore trattamento dei dati ottenuti in questo modo, che comporta un intervento autonomo (vedi BVerfGE 100, 313 <366 f.>). Inoltre, la Sezione 7 (2) BNDG regola le restrizioni sulla raccolta dei dati e crea quindi il diritto legale ache la raccolta di dati dall'estero è consentita senza ulteriori basi giuridiche. Di conseguenza, la Sezione 7, paragrafi 1 e 2, BNDG intende anche legittimare la raccolta di dati da parte del Servizio di intelligence federale dall'estero.

D.

121

Questa interferenza con i diritti fondamentali non è giustificata costituzionalmente. Le disposizioni che le autorizzano non soddisfano già i requisiti costituzionali per le autorizzazioni di interferire con i diritti fondamentali in questione. Possono contare su un'adeguata base di competenze. Tuttavia, violano il requisito di citazione dell'articolo 19.1 frase 2 della Legge fondamentale.

IO.

122

Non ci sono preoccupazioni costituzionali fondamentali riguardo alla competenza legislativa. Il legislatore federale può basare le disposizioni contestate sull'articolo 73.1 n. 1 GG.

123

1. La base di competenza pertinente è l'articolo 73.1 n. 1 GG, che stabilisce la competenza legislativa del governo federale in materia di affari esteri e difesa.

124

a) L'istituzione di un organismo per l'informazione globale all'estero è indiscutibilmente una questione di affari esteri ai sensi dell'articolo 73, paragrafo 1, n. 1 della legge di base (cfr. BVerfGE 100, 313 <369>). Ciò include anche dotarli di poteri adeguati. Tuttavia, i compiti che i legislatori possono delegare a tale organo sono limitati.

125

aa) Il concetto di affari esteri di cui all'articolo 73 capoverso 1 n. 1 GG non può essere determinato senza riguardo alla distribuzione dei poteri legislativi. Da un lato, non deve essere interpretato in modo tale da compromettere la divisione dei poteri tra il governo federale e quello statale. D'altra parte, deve adattarsi ai vari incarichi di competenza al governo federale. Da entrambi i punti di vista, non si comprende il termine, secondo il quale tutti i fatti relativi a paesi stranieri vengono considerati affari esteri. Ciò include quelle domande che sono importanti per le relazioni della Repubblica Federale Tedesca con altri stati o istituzioni intergovernative, in particolare per la progettazione della politica estera (vedi BVerfGE 100, 313 <368 f.>; Vedi anche BVerfGE 133, 277 <319 marg.101>).

126

È necessario operare una distinzione tra la competenza legislativa ai sensi dell'articolo 73 capoverso 1 n. 1 GG e la competenza legislativa ai sensi dell'articolo 73 capoverso 1 n. 9a GG, che conferisce al governo federale la competenza legislativa unicamente per la difesa contro i pericoli del terrorismo internazionale in relazione all'Ufficio federale di polizia criminale concesso. Nella zona di frontiera per la lotta contro la criminalità, è anche importante che l'articolo 73, paragrafo 1, n. 10 della legge di base conferisca alla Confederazione taluni poteri legislativi, e allo stesso tempo limitati, per la cooperazione tra la Federazione e i Länder nel campo della polizia criminale, per l'istituzione di un Ufficio federale di polizia criminale e per il diritto internazionale Assegna la lotta al crimine. Ciò non significa che la lotta contro i crimini internazionali, ma la lotta internazionale contro i crimini,Ad esempio, la cooperazione tra autorità tedesche e straniere in materia di polizia criminale. Per inciso, la legge di polizia è di competenza degli stati federali come legge di sicurezza (vedi BVerfGE 100, 313 <369>).

127

bb) Ciò significa che il governo federale non può generalmente affidare al Servizio di intelligence federale informazioni di intelligence straniera allo scopo di garantire la sicurezza interna. L'articolo 73.1 frase 1 della Legge fondamentale non autorizza il legislatore federale a conferire poteri volti a

prevenire, prevenire o perseguire i reati in quanto tali (cfr. BVerfGE 100, 313 <370>; 133, 277 <319 marg 101>). A tal fine, al Servizio di intelligence federale possono essere assegnati solo compiti e poteri che hanno un significato di politica estera e di sicurezza e quindi hanno una dimensione internazionale.

128

Al contrario, ciò non limita il legislatore federale ad affidare al Servizio di intelligence federale il compito di fornire al governo federale le basi decisionali per garantire la sua capacità di politica estera o di difesa di agire (vedi BVerfGE 100, 313 <368 ss.>). Questo è il compito principale dell'intelligence straniera, da cui deve essere modellato anche il profilo generale del servizio basato sull'articolo 73.1 n. 1 della Legge fondamentale. Tuttavia, al servizio di intelligence federale può essere affidato anche il compito di individuare tempestivamente minacce dall'estero se presentano una dimensione sufficientemente internazionale. Il fattore decisivo è che si tratta di pericoli,che, per loro natura e peso, possono avere un impatto sulla posizione della Repubblica Federale nella comunità internazionale e sono particolarmente importanti in termini di politica estera e di sicurezza in questo senso. Ad esempio, vi sono pericoli rappresentati da potenti reti criminali organizzate a livello internazionale, da attacchi informatici controllati esternamente su importanti infrastrutture o da atti di terrorismo che sono espressione di situazioni di conflitto interconnesse a livello internazionale. Al contrario, la competenza non include la creazione di regolamenti per indagare sui reati individuali, anche significativi, a livello nazionale, semplicemente perché ci sono contributi o fonti di conoscenza all'estero.La responsabilità del servizio di intelligence federale non può in genere essere estesa alle indagini sui reati stranieri ai sensi della sezione 6 del codice penale. Il fatto che il reato all'estero sia punibile qui e che tali norme siano incluse negli accordi internazionali non giustifica di per sé il fatto che il loro chiarimento abbia in ogni caso un significato di politica estera e di sicurezza, che da solo conferisce alla Confederazione competenza legislativa ai sensi dell'articolo 73 capoverso 1 n. 1 GG aperto.

129

b) Le disposizioni contestate possono quindi basarsi sulla competenza legislativa dell'articolo 73.1 n. 1 GG. Questo inizialmente si applica alla Sezione 6 BNDG. La sezione 6 (1) n. 1 BNDG apre l'uso della sorveglianza strategica non solo per identificare le minacce alla sicurezza esterna, ma anche per identificare le minacce alla sicurezza interna. Tuttavia, questo è incluso nella restrizione del § 6 BNDG a tutti i compiti del Servizio di intelligence federale che abbraccia tutti i fatti. Questo vale sia per il numero 1 che per il numero 2 e il numero 3, e quindi anche per il profilo professionale del governo federale. Le misure di sorveglianza in conformità con la Sezione 6 (1) BNDG sono quindi ammissibili solo per acquisire conoscenze su paesi stranieri che sono di importanza politica estera e di sicurezza (Sezione 1 (2) BNDG). Ai sensi dell'articolo 73 capoverso 1 n.1 GG è innocuo in termini di competenza, ma presuppone un'interpretazione e un trattamento del regolamento che tenga conto dei limiti stabiliti dal diritto della competenza. In particolare, i poteri non possono quindi essere utilizzati senza restrizioni come base per i servizi per le autorità di sicurezza interna, neppure quando il governo federale emette un ordine.

130

Nient'altro si applica a § 7 e §§ da 13 a 15 BNDG. Questi regolamenti sono anche vincolati alla definizione di attività di § 1 Abs. 2 BNDG e limitati da essi. Il fatto che §§ da 13 a 15 BNDG apre anche la sorveglianza per acquisire conoscenze nell'interesse di altri stati nell'ambito della cooperazione non cambia nulla in base al diritto di competenza. L'assegnazione di tale regolamento agli "affari esteri" è fuori dubbio.

131

La responsabilità del governo federale di regolare la trasmissione delle conoscenze acquisite dalle misure di sorveglianza di § 24 BNDG risulta dal contesto fattuale dell'articolo 73 capoverso 1 n. 1 GG come base di competenza applicabile per la raccolta dei dati (cfr. BVerfGE 125, 260 <314 >; 133, 277 <319 f. Margine 101>).

132

2. Al contrario, i regolamenti impugnati non possono essere basati su altri titoli di competenza. Ciò vale in particolare per l'articolo 73 capoverso 1 n. 10 GG e la competenza federale ivi regolamentata per la lotta internazionale alla criminalità.

133

Per quanto riguarda §§ 6, 7 BNDG, questo è già escluso perché non regolano la cooperazione internazionale (vedi BVerfGE 100, 313 <368 f.>). Nient'altro vale anche per le sezioni da 13 a 15 BNDG. Questi regolamenti riguardano le forme di cooperazione internazionale. Tuttavia, non regolano il coordinamento della lotta contro la criminalità, ma piuttosto un ampliamento dei poteri del Servizio di intelligence federale di raccogliere, valutare e trasmettere dati al fine di essere in grado di raccogliere gli interessi di informazione di altri servizi. Di conseguenza, il legislatore federale si è basato esclusivamente sull'articolo 73, paragrafo 1, n. 1 GG per la creazione delle sezioni 13-15 BNDG (cfr. BTDrucks 18/9041, p. 19). Ciò lascia la questione fondamentale se l'articolo 73 capoverso 1 n.10 GG garantisce al governo federale il potere di regolare la lotta alla criminalità internazionale in generale - e quindi di escludere gli stati federali in generale - o se concede al governo federale questa competenza normativa solo in relazione alla progettazione dei poteri dell'Ufficio federale di polizia criminale (cfr. Becker, DÖV 2011, pag. 840 <847>; Zöller, in: Roggan / Kutscha, Manuale sulla legge sulla sicurezza interna, 2 ° ed. 2006, p. 447 <459>; vedi anche Uhle, in: Maunz / Dürig, GG, Art. 73 marg 255 [ottobre 2019]; sulla genesi di Schneider, Das Grundgesetz, documentazione della sua creazione, vol. 17, 2007, p. 905 ss.).o se conferisce al governo federale solo questa competenza normativa in relazione alla progettazione dei poteri dell'Ufficio federale di polizia criminale (cfr. Becker, DÖV 2011, p. 840 <847>; Zöller, in: Roggan / Kutscha, Handbuch zum Recht der Internal Sicherheit, 2. Ed. 2006, p. 447 <459>; vedi anche Uhle, in: Maunz / Dürig, GG, Art. 73 Paragrafo 255 [ottobre 2019]; sulla storia della storia Schneider, Das Grundgesetz, documentazione della sua creazione, Vol. 17, 2007, p. 905 ss.).o se conferisce al governo federale solo questa competenza normativa in relazione alla progettazione dei poteri dell'Ufficio federale di polizia criminale (cfr. Becker, DÖV 2011, p. 840 <847>; Zöller, in: Roggan / Kutscha, Handbuch zum Recht der Internal Sicherheit, 2. Ed. 2006, p. 447 <459>; vedi anche Uhle, in: Maunz / Dürig, GG, Art. 73 Paragrafo 255 [ottobre 2019]; sulla storia della storia Schneider, Das Grundgesetz, documentazione della sua creazione, Vol. 17, 2007, p. 905 ss.).

II.

134

Le disposizioni contestate sono, tuttavia, formalmente incostituzionali perché violano il requisito di citazione dell'articolo 19.1 frase 2 della Legge fondamentale (cfr. Huber, ZRP 2016, p. 162 <163>; Hölscheidt, Jura 2017, p. 148 < 155>; Marxsen, DÖV 2018, p. 218 <225>; Dietrich, in: Schenke / Graulich / Ruthig [ed.], Sicherheitsrecht des Bundes, 2a edizione 2019, § 6 BNDG Rn.11). Il Federal Intelligence Service Act menziona l'articolo 10 capoverso 1 GG per quanto riguarda gli interventi ai sensi del § 3 BNDG (cfr. Il paragrafo 3 ivi), ma non per gli interventi ai sensi delle

normative controverse qui. Il fatto che il requisito della citazione non sia rispettato non può essere giustificato dal fatto che i regolamenti impugnati adottano una prassi amministrativa di vecchia data e ora la regolano per la prima volta. In particolare, non si può fare riferimentoche la citazione non si applica se la legge limita le restrizioni esistenti in materia di diritti fondamentali invariate o con lievi deviazioni (vedere BVerfGE 35, 185 <188 f.>). Dopotutto, la pratica amministrativa senza legge non è né la legge applicabile né una limitazione dei diritti fondamentali e, a differenza delle leggi parlamentari che rispettano il requisito della citazione, non si basa su valutazioni già fatte dal legislatore parlamentare. La funzione di avvertimento del requisito di citazione non è sostituita da una semplice pratica amministrativa. Questo vale soprattutto per la pratica segreta di un servizio di notizie.Dopotutto, la pratica amministrativa senza legge non è né la legge applicabile né una limitazione dei diritti fondamentali e, a differenza delle leggi parlamentari che rispettano il requisito della citazione, non si basa su valutazioni già fatte dal legislatore parlamentare. La funzione di avvertimento del requisito di citazione non è sostituita da una semplice pratica amministrativa. Questo vale soprattutto per la pratica segreta di un servizio di notizie.Dopotutto, la pratica amministrativa senza legge non è né la legge applicabile né una limitazione dei diritti fondamentali e, a differenza delle leggi parlamentari che rispettano il requisito della citazione, non si basa su valutazioni già fatte dal legislatore parlamentare. La funzione di avvertimento del requisito di citazione non è sostituita da una semplice pratica amministrativa. Questo vale soprattutto per la pratica segreta di un servizio di notizie.

135

Piuttosto, l'obbligo di quotazione viene violato se, sulla base di una certa interpretazione dell'area di protezione - come il presupposto che il potere statale tedesco non sia vincolato da diritti fondamentali nel caso di atti che colpiscono gli stranieri all'estero - il legislatore non ritiene che i diritti fondamentali vengano lesi. Perché allora manca la consapevolezza del legislatore di autorizzare interventi sui diritti fondamentali e della sua volontà di giustificarne gli effetti, che è il punto del principio di citazione (cfr. BVerfGE 85, 386 <404>; 113, 348 <366>; 129, 208 <236 f.>). Inoltre, il legislatore elude il dibattito pubblico in cui è necessario chiarire la necessità e la portata dell'interferenza con i diritti fondamentali (cfr. BVerfGE 85, 386 <403 f.>; 129, 208 <236 f.>).

E.

136

Inoltre, i regolamenti impugnati non sono materialmente compatibili con la legge fondamentale. La Legge fondamentale non è fondamentalmente in conflitto con lo strumento di sorveglianza strategica e la relativa cooperazione con altri servizi di intelligence. Tuttavia, i regolamenti non soddisfano i requisiti centrali derivanti dai diritti fondamentali.

IO.

137

1. Gli interventi di cui all'articolo 10 capoverso 1 GG e anche all'articolo 5 capoverso 1 frase 2 GG - come gli interventi in tutti i diritti fondamentali - devono basarsi su un'autorizzazione legale che soddisfi i requisiti di chiarezza delle norme e il principio di certezza (cfr. BVerfGE 65, 1 <44; 54>; 100, 313 <359 f.>; StRspr). La chiarezza delle norme e la certezza delle autorizzazioni per la raccolta e l'elaborazione segrete di dati personali sono generalmente soggette a requisiti più elevati, poiché l'elaborazione dei dati avviene inosservata dalle persone interessate e pertanto i poteri non possono essere concretizzati nell'interazione dei singoli ordini amministrativi e controllo giudiziario

(vedi BVerfGE 141, 220 <265 paragrafo 94>; vedi anche EGMR, Big Brother Watch e altri c. Regno Unito, sentenza del 13 settembre 2018, n. 58170/13 e altri, § 306).

138

Questo non fa eccezione per i servizi di intelligence. Anche se In larga misura, i loro doveri devono essere tenuti segreti. Le informazioni all'estero, in particolare, si basano su una rigorosa schermatura per poter ottenere informazioni senza mettere in pericolo le proprie risorse e fonti (vedere BVerfGE 30, 1 <18 f.>; 100, 313 <397 f.>). Non solo devono essere mantenute segrete le singole misure e conclusioni del Servizio federale di intelligence incaricato, ma anche informazioni sulla misura in cui il servizio è possibile o impossibile da chiarire e il livello di dettaglio che raggiunge. Poiché il servizio deve presumere che sia esso stesso esposto a tentativi di ricerca di servizi stranieri, i requisiti di riservatezza continuano a essere profondi nell'organizzazione dei servizi. Il legislatore può tenerne conto.

139

Tuttavia, non si può dedurre dalla necessità di riservatezza dell'intelligence straniera che poco si sa circa il Servizio federale di intelligence e che la sua base giuridica dovrebbe rimanere il più possibile al buio. Nello stato costituzionale democratico, non può esserci alcun principio di segretezza riguardo alle basi di azione e ai limiti dei poteri di intelligence. Proprio come il bilancio generale e la forza del personale dei servizi di intelligence devono essere pienamente determinati dal parlamento ed essere pubblicamente responsabili (per il controllo della gestione dei fondi in dettaglio, vedere § 10a BHO), anche i loro poteri devono essere regolati dalla legge in modo standardizzato e determinato di fronte al pubblico e alle responsabilità chiaramente assegnato (vedi Gusy, in:Schenke / Graulich / Ruthig [ed.], Legge federale sulla sicurezza, 2a edizione 2019, prep. BNDG Marg. 10, 13). Il vincolo dei diritti fondamentali corrisponde alla responsabilità parlamentare-democratica per la limitazione dei diritti fondamentali. A questo proposito, la riservatezza si applica solo in conformità con il diritto pubblico. Inoltre, non è fine a se stesso per l'intelligence straniera, ma è giustificato solo se il tipo e la portata dell'attività del servizio che richiede riservatezza sono legittimati in modo democratico e pubblico e la riservatezza rimane entro i limiti specifici della necessità funzionale.A questo proposito, la riservatezza si applica solo in conformità con il diritto pubblico. Inoltre, non è fine a se stesso per l'intelligence straniera, ma è giustificato solo se il tipo e la portata dell'attività del servizio che richiede riservatezza sono legittimati in modo democratico e pubblico e la riservatezza rimane entro i limiti specifici della necessità funzionale.A questo proposito, la riservatezza si applica solo in conformità con il diritto pubblico. Inoltre, non è fine a se stesso per l'intelligence straniera, ma è giustificato solo se il tipo e la portata dell'attività del servizio che richiede riservatezza sono legittimati in modo democratico e pubblico e la riservatezza rimane entro i limiti specifici della necessità funzionale.

140

Il requisito di una versione chiara e sufficientemente definita dei poteri legali non mette a repentaglio la possibilità di gestirli segretamente in materia. Poiché i poteri creano solo possibilità giuridiche astratte, non dicono nulla sul se, come, con quale scopo e con quale successo vengono utilizzati.

141

2. Le disposizioni contestate possono essere giustificate come autorizzazioni di violazione del segreto delle telecomunicazioni e della libertà di stampa se sono conformi al principio di

proporzionalità. Devono quindi perseguire uno scopo legittimo, essere idonei a raggiungere lo scopo, essere necessari ed essere proporzionati in senso stretto (cfr. VerfGE 67, 157 <173>; 120, 378 <427>; 141, 220 <265 para. 93>; stRspr). Per le misure di sorveglianza segreta da parte delle autorità di sicurezza, la Corte costituzionale federale ha specificato i requisiti risultanti in una varietà di decisioni e le ha sintetizzate in particolare nella decisione sulla legge federale sulla polizia criminale (vedi BVerfGE 141, 220 <268 ss. Rn. 103 ss.>). Tali norme, che si applicano anche alle misure di sorveglianza dell'intelligence,costituisce il punto di partenza per i requisiti per la raccolta e l'elaborazione dei dati nonché per i requisiti per la trasmissione dei dati. Tuttavia, lo strumento di sorveglianza strategica come mezzo speciale di intelligence straniera non è stato ancora preso in considerazione con loro. In relazione alla decisione sui poteri di controllo strategico ai sensi dell'articolo 10 della legge (cfr. BVerfGE 100, 313 <368 segg.>), Devono pertanto essere specificati.In relazione alla decisione sui poteri di controllo strategico ai sensi dell'articolo 10 della legge (cfr. BVerfGE 100, 313 <368 segg.>), Devono pertanto essere specificati.In relazione alla decisione sui poteri di controllo strategico ai sensi dell'articolo 10 della legge (cfr. BVerfGE 100, 313 <368 segg.>), Devono pertanto essere specificati.

II.

142

L'autorizzazione alla raccolta e al trattamento dei dati sotto forma di sorveglianza strategica delle telecomunicazioni è, in quanto strumento speciale di intelligence straniera, compatibile in linea di principio con l'articolo 10.1 della Legge fondamentale (1.). Tuttavia, ciò richiede un design sufficientemente limitante (2.).

143

1. La concessione del diritto all'intelligence straniera attraverso la sorveglianza strategica delle telecomunicazioni non è esclusa dall'inizio dall'articolo 10.1 della Legge fondamentale. Sebbene non si limiti a eventi specifici determinati oggettivamente e dia quindi diritto a gravi violazioni dei diritti fondamentali senza una soglia di intervento, può essere giustificato dallo scopo dell'intelligence straniera e dalle sue speciali condizioni di azione con una struttura sufficientemente limitata prima dell'articolo 10.1 della Legge fondamentale e il principio di proporzionalità.

144

a) La sorveglianza strategica delle telecomunicazioni ha uno scopo legittimo ed è adeguata e necessaria per raggiungerla sulla base del principio di proporzionalità. Secondo la volontà del legislatore, la sorveglianza strategica dovrebbe fornire informazioni su paesi stranieri che hanno un significato di politica estera e di sicurezza per la Repubblica Federale. Ha lo scopo di aiutare a identificare i pericoli in una fase precoce, preservare la capacità della Repubblica federale di agire e fornire al governo federale informazioni su questioni di politica estera e di sicurezza. Questo è un obiettivo legittimo. La sorveglianza strategica delle telecomunicazioni è anche un mezzo adeguato per farlo perché consente l'accesso a tali informazioni. I dati sono inizialmente registrati su larga scala,che non hanno contenuti informativi pertinenti non cambia il fatto che la registrazione e la valutazione complessive dei flussi di dati possono portare a risultati significativi. Il monitoraggio strategico soddisfa anche i requisiti di necessità. Senza l'acquisizione ampia e senza eventi dei flussi di dati e la loro valutazione, non è possibile ottenere le informazioni corrispondenti. Un mezzo meno intensivo di intervento, che in genere garantiva informazioni comparabili, non è evidente.Senza l'acquisizione ampia e senza eventi dei flussi di dati e la loro valutazione, non è possibile ottenere le informazioni corrispondenti. Un mezzo meno intensivo di intervento, che in

genere garantiva informazioni comparabili, non è evidente.Senza l'acquisizione ampia e senza eventi dei flussi di dati e la loro valutazione, non è possibile ottenere le informazioni corrispondenti. Un mezzo meno intensivo di intervento, che in genere garantiva informazioni comparabili, non è evidente.

145

b) L'autorizzazione del Servizio di intelligence federale a monitorare strategicamente le telecomunicazioni degli stranieri all'estero può essere giustificata in linea di principio in termini di proporzionalità in senso stretto prima dell'articolo 10.1 della Legge fondamentale.

146

aa) Tuttavia, la sorveglianza strategica delle telecomunicazioni è uno strumento con un peso di intervento particolarmente elevato.

147

(1) Gli interventi aperti con lei inizialmente pesano molto perché sono utilizzati per penetrare segretamente nelle relazioni personali di comunicazione che sono spesso private e, in determinate circostanze, altamente confidenziali. Una tale sorveglianza segreta delle telecomunicazioni significa sostanzialmente un intervento serio (vedi BVerfGE 141, 220 <264 f. Rn. 92>), indipendentemente dal fatto che la sorveglianza avvenga a livello nazionale o all'estero o riguardi residenti, tedeschi o stranieri.

148

(2) In relazione alla sorveglianza delle singole telecomunicazioni, tuttavia, la sorveglianza strategica ha un impatto minore in quanto si riferisce a flussi di dati la cui produttività non può essere prevista in dettaglio. Inoltre, nella misura in cui è finalizzato al monitoraggio di singole persone mediante termini di ricerca formali, è in genere meno preciso e incompleto, poiché le reti e i collegamenti di trasmissione (il cosiddetto instradamento) utilizzati per una specifica connessione di comunicazione sono in gran parte determinati spontaneamente, a seconda della disponibilità, e solo una piccola parte del Vengono registrate reti di accordi di rete esistenti in Germania e nel mondo. Il monitoraggio strategico differisce nel suo peso di intervento almeno in linea di principio da una restrizione nei singoli casi,come è reso possibile dal § 3 G 10.

149

(3) Inoltre, il peso dell'intervento contro le persone che risiedono all'estero è ridotto dal fatto che la sorveglianza non è sempre finalizzata a conseguenze operative immediate allo stesso modo delle misure di sorveglianza contro i tedeschi o le persone residenti in Germania. L'intelligence straniera riguarda processi in altri paesi in cui lo stato tedesco non ha poteri sovrani ed è riservato al Servizio di intelligence federale in quanto autorità che generalmente non ha poteri operativi propri. Il compito principale delle informazioni all'estero è innanzitutto quello di creare una base di informazioni, valutare le informazioni, verificarne la pertinenza e quindi renderle disponibili al governo federale e, se necessario, ad altri destinatari.Tuttavia, anche qui la sorveglianza è spesso collegata all'obiettivo di adottare misure contro le persone colpite - possibilmente in scambio di conoscenze con altri paesi - e quindi rimane importante. Tuttavia, il Servizio federale di intelligence non può adottare tali misure contro le persone all'estero. Le misure che altri organismi adottano nei confronti delle persone colpite sulla base di tali informazioni dipendono dal trasferimento dei dati,

che può e deve essere giuridicamente limitato dal principio di ipotetica raccolta di dati (v. Punti 216 e seguenti e 220 e seguenti. Di seguito).Tuttavia, il Servizio federale di intelligence non può adottare tali misure contro le persone all'estero. Le misure che altri organismi adottano nei confronti delle persone colpite sulla base di tali informazioni dipendono dal trasferimento dei dati, che può e deve essere giuridicamente limitato dal principio di ipotetica raccolta di dati (v. Punti 216 e seguenti e 220 e seguenti. Di seguito).Tuttavia, il Servizio federale di intelligence non può adottare tali misure contro le persone all'estero. Le misure che altri organismi adottano nei confronti delle persone colpite sulla base di tali informazioni dipendono dal trasferimento dei dati, che può e deve essere giuridicamente limitato dal principio di ipotetica raccolta di dati (v. Punti 216 e seguenti e 220 e seguenti. Di seguito).

150

(4) Al contrario, la straordinaria gamma di sorveglianza strategica delle telecomunicazioni è particolarmente difficile. È consentito a ogni persona senza motivo ed è infine guidato esclusivamente da determinati scopi. Non sono richieste soglie di intervento oggettivo in relazione a situazioni limitanti né per le persone interessate dalla sorveglianza. L'autorità abilitata in questo modo può solo decidere liberamente su quali reti, dati e persone dovrebbe indirizzare le misure nell'ambito di scopi astratti.

151

Tale autorizzazione ha una portata straordinaria, soprattutto nelle attuali condizioni della tecnologia dell'informazione e la sua importanza per le relazioni di comunicazione. L'intensità della sua interferenza non può più essere paragonata ai poteri che la Corte costituzionale federale ha dovuto decidere nella sua decisione di monitorare strategicamente le comunicazioni interne-straniere nel 1999. A quel tempo, la sorveglianza delle telecomunicazioni era effettivamente limitata in termini di apparecchiature di telecomunicazione utilizzate in situazioni specifiche (cfr. BVerfGE 100, 313 <379 f.>), Ma oggi vengono registrati volumi di dati incomparabilmente più grandi. Sono utilizzati per trasportare un numero inconfondibile di forme di comunicazione elettronica e per valutarle.Alla luce dell'uso diffuso e variegato dei servizi di comunicazione, ogni tipo di azione individuale e interazione interpersonale si riflette sempre più nei segnali elettronici, rendendolo accessibile alla sorveglianza delle telecomunicazioni. La sorveglianza cattura così in profondità tutti i giorni, anche i processi di comunicazione altamente privati e spontanei, incluso lo scambio di immagini e documenti. Tecnicamente, anche oggi è possibile monitorare il comportamento degli utenti sul World Wide Web e gli interessi, i desideri e le preferenze qui espressi. Allo stesso tempo, le opzioni di analisi ora vanno molto oltre. Nel 1999 il Servizio di intelligence federale mancava ancora delle possibilità tecniche di riconoscimento vocale automatico,I programmi per il riconoscimento vocale, la traduzione o il riconoscimento delle immagini sono già disponibili al pubblico oggi. Nel complesso, la sorveglianza strategica delle telecomunicazioni ora si estende potenzialmente a quasi tutte le comunicazioni, compresa la società civile (cfr. Il valore informativo dei dati sul traffico BVerfGE 125, 260 <319>; sulle opzioni di riconoscimento ampliato dei servizi di intelligence di Omand, in: Dietrich / Sule [ed.], Legge e politiche sull'intelligence in Europa, 2019, p. 38 <margine n. 37 ss.>).sulla rilevanza dei dati sul traffico BVerfGE 125, 260 <319>; sulle maggiori possibilità di riconoscimento dei servizi di intelligence Omand, in: Dietrich / Sule [ed.], Intelligence Law and Policies in Europe, 2019, p. 38 <marg. 37 e seguenti>).sulla rilevanza dei dati sul traffico BVerfGE 125, 260 <319>; sulle maggiori possibilità di riconoscimento dei servizi di intelligence Omand, in: Dietrich / Sule [ed.], Intelligence Law and Policies in Europe, 2019, p. 38 <marg. 37 e seguenti>).

152

(5) La sorveglianza strategica delle telecomunicazioni ha un impatto particolare in quanto consente anche una sorveglianza personale mirata. Ciò apre una dimensione propria rispetto ai poteri che sono stati oggetto della decisione del Senato del 1999. Mentre la sorveglianza strategica è apparsa lì solo nella misura in cui ha funzionato con termini di ricerca specifici senza riferimenti personali specifici (vedere BVerfGE 100, 313 <384>), la ricognizione strategica delle telecomunicazioni, come è in discussione qui, opera principalmente con termini di ricerca formale come gli identificatori di telecomunicazione, che consentono anche di sorvegliare in modo specifico la telecomunicazione delle singole persone.Ciò fornisce un chiarimento strategico sulle telecomunicazioni un ambito di intervento sostanzialmente più ampio e si avvicina alla sorveglianza individuale delle telecomunicazioni.

153

(6) In relazione alla precedente situazione giuridica, vi è un ulteriore onere che il monitoraggio strategico ora apra anche una certa quantità di archiviazione dei dati sul traffico in una certa misura. Attraverso la loro valutazione - sempre senza alcuna motivazione e unicamente guidata - si possono ottenere approfondimenti sulla comunicazione e sul comportamento delle persone in movimento, che possono andare ben oltre la valutazione del contenuto del traffico di comunicazione individuale (cfr. Il valore informativo di tali dati BVerfGE 125, 260 <319> ; CGUE, sentenza dell'8 aprile 2014, Digital Rights Ireland e Seitlinger et al., C-293/12, C-594/12, EU: C: 2014: 238, punti 48, 56). Ciò aumenta anche considerevolmente il peso dell'incarico.

154

bb) Nonostante il peso di intervento particolarmente pesante della sorveglianza strategica, ciò può essere giustificato costituzionalmente come un'autorizzazione specifica per l'intelligence straniera.

155

(1) Tuttavia, la rinuncia a qualsiasi soglia di intervento concreta è un'esenzione da un elemento fondamentale dei requisiti dello Stato di diritto, che è essenziale, in particolare per quanto riguarda le agenzie di sicurezza nazionali, per un uso meno intensivo dell'intervento, ma ancora di più per gravi interferenze con i diritti fondamentali come la sorveglianza delle telecomunicazioni (cfr. BVerfGE 141, 220 <269 e seguenti. Paragrafo 104 e seguenti>; 150, 244 <280 e seguenti. Paragrafo 90 e seguenti>). Il requisito di una soglia di intervento basata su circostanze specifiche garantisce che gli interventi sui diritti fondamentali siano limitati, li vincoli a condizioni oggettivate e consenta il controllo basato su criteri autonomi. Un'autorizzazione finale e un'autorizzazione limitata per tali interventi sono fondamentalmente incompatibili con l'articolo 10.1 della Legge fondamentale.

156

In linea di principio, ciò vale anche per i servizi di informazione. Nella misura in cui le misure di sorveglianza si estendono alla comunicazione interna, sono richieste soglie di intervento solide conformemente ai requisiti generali. Non è diverso se a determinate persone, sia in Germania che all'estero, viene ordinato di attuare misure di sorveglianza sotto forma di sorveglianza delle telecomunicazioni o ricerca online (vedere BVerfGE 120, 274 <326 e seguenti>; 125, 260 <320 ss.>; 141, 220 <270 ss. Marginale 106 ss.>; Vedere anche § 3 G 10).

157

(2) La situazione è diversa per l'intelligence dell'intelligence all'estero, nella misura in cui è finalizzata alla raccolta di informazioni generali per informare il governo federale o - in anticipo delle restrizioni individuali in singoli casi - a un preavviso. Qui, il legislatore può anche fornire al Servizio di intelligence federale lo strumento di sorveglianza strategica delle telecomunicazioni. Per quanto riguarda questo specifico compito, il fatto che questo sia essenzialmente finalizzato e limitato non è incompatibile con i requisiti di proporzionalità fin dall'inizio (anche per il monitoraggio strategico delle telecomunicazioni internazionali BVerfGE 100, 313 <373 ss.>).

158

(a) Il punto di partenza per questo è il profilo dei compiti dell'intelligence straniera. Non si tratta principalmente di indagini mirate su processi già stabiliti e quindi non di chiarire fatti già chiaramente definiti, ma soprattutto di trovare e identificare informazioni rilevanti in merito a interessi di conoscenza che possono essere determinati solo in modo astratto. A tale proposito, il compito delle informazioni all'estero è innanzitutto quello di creare una base di informazioni completa al fine di monitorare gli sviluppi su una vasta area, quindi valutare le informazioni, verificarne la pertinenza e infine renderle disponibili in forma abbreviata al governo federale e, se necessario, ad altri destinatari.I potenziali interessi cognitivi aprono un ampio spettro con la loro attenzione sull'intera politica estera e di sicurezza.

159

(b) Per questo compito, una ricognizione occasionale, essenzialmente controllata esclusivamente sotto forma di monitoraggio strategico può essere giustificata costituzionalmente. Contrariamente alle misure per l'identificazione precoce dei pericoli all'interno del paese, è di primaria importanza che le informazioni fornite all'estero mirino a chiarire e comprendere le circostanze per le quali vi è una mancanza di consapevolezza quotidiana immediata da parte delle autorità tedesche e del pubblico nazionale. Lo scopo è quello di ottenere approfondimenti sugli sviluppi in contesti che sono difficili da interpretare con le informazioni solo all'interno della Germania, e in alcuni casi interessano paesi con strutture non molto aperte in termini di informazioni. Soprattutto, tuttavia, sono le condizioni speciali per l'azione durante l'esecuzione di questo compito.L'intelligence straniera si riferisce a processi in altri paesi in cui lo stato tedesco è e può essere presente a volte con le proprie fonti di conoscenza e in cui non ha poteri sovrani che gli danno accesso diretto alle informazioni (anche EGMR, Big Brother Watch e altri v Regno Unito, sentenza del 13 settembre 2018, n. 58170/13 e altri, § 518). Nell'interesse della capacità di agire e di sicurezza della Repubblica Federale Tedesca, le informazioni devono in particolare essere in grado di ottenere informazioni che possono - eventualmente con intenzionalità intenzionale - negare e che sono mantenute segrete nella sfera sovrana del paese terzo. Ai sensi della legge del paese di destinazione, le misure di informazione possono spesso essere illegali o, almeno, spesso indesiderabili.Allo stesso tempo, il servizio si confronta con le attività di controspionaggio dei paesi target, che a loro volta ostacolano e cercano di impedire le indagini per mezzo di polizia e intelligence. Il lavoro è quindi particolarmente vulnerabile e precario ed è riferito a mezzi straordinari.

160

Allo stesso tempo, si dovrebbe tenere presente che l'illuminazione non è solo faccia a faccia con i vari servizi di intelligence, ma anche in cooperazione tra loro per illuminare le questioni relative alla Repubblica Federale Tedesca e ad altri paesi. In particolare, il chiarimento di eventi politicamente o militarmente rilevanti, che serve solo a informare il governo federale, ma anche il chiarimento precoce dei pericoli della criminalità internazionale, che comprende anche il terrorismo internazionale, oggi dipende dalla cooperazione tra i servizi per essere efficaci. Tuttavia, il servizio

di intelligence federale è in grado di cooperare solo se dispone anche di poteri con cui può controllare i risultati di altri servizi,può assorbirli e usarli ulteriormente e con il loro aiuto può anche contribuire come partner attraverso le proprie conoscenze. Le autorizzazioni per la sorveglianza indiscriminata delle comunicazioni straniere sono, secondo quanto è noto, ora parte dell'attrezzatura diffusa di questi servizi (per gli Stati Uniti: Sezione 702 Foreign Intelligence Surveillance Act; cfr. Renan, in: Goldman / Rascoff [ed.], Global Intelligence Oversight, 2016, p. 121 <esp. 123 ss.>; Per il Regno Unito Parte 6 Capitolo 1 Investigatory Powers Act 2016; vedi Leigh, in: Dietrich / Sule [ed.], Legge e politiche sull'intelligence in Europa , 2019, p. 553 e seguenti; McKay / Walker, in: Dietrich / Gärditz / Graulich / Gusy / Warg [ed.], Riforma dei servizi di intelligence tra legalizzazione e internazionalizzazione, 2019, p. 119 e seguenti; per la Francia:Articoli da L854-1 a L854-9 Codice della sicurezza interna [Messaggi di sorveglianza delle comunicazioni elettroniche internazionali]; S. anche Le Divelec, in: Dietrich / Sule [ed.], Legge e politiche sull'intelligence in Europa, 2019, p. 516 e seguenti; Warusfel, in: Dietrich / Gärditz / Graulich / Gusy / Warg [ed.], Riforma dei servizi di intelligence tra legalizzazione e internazionalizzazione, 2019, p. 129 ss.).

161

(c) deve essere preso in considerazione anche l'interesse pubblico eccezionale per informazioni efficaci all'estero.

162

Conformemente al collegamento competente (sopra, nm. 123 e seguenti), l'intelligence straniera mira sempre a informazioni importanti per la posizione e la capacità della Germania di agire nella comunità internazionale e che pertanto rivestono un'importanza di politica estera e di sicurezza in questo senso. Fornire informazioni al governo federale per le sue decisioni in materia di politica estera e di sicurezza lo aiuta ad affermarsi nel campo politico del potere delle relazioni internazionali e può prevenire gravi decisioni sbagliate. A questo proposito, si tratta indirettamente della conservazione dell'autodeterminazione democratica e della protezione dell'ordine costituzionale - e quindi dei beni costituzionali di alto rango. Vi è quindi una questione di interesse nazionaleciò va ben oltre l'interesse a garantire la sicurezza interna in quanto tale.

163

È importante qui che nel corso dello sviluppo della tecnologia dell'informazione e della comunicazione internazionale, nonché della più stretta integrazione transfrontaliera delle condizioni di vita in generale, le minacce dall'estero sono aumentate considerevolmente. Anche la diagnosi precoce di situazioni pericolose che minacciano dall'estero è di particolare importanza per la sicurezza. L'espansione e l'internazionalizzazione delle opzioni di comunicazione e l'accresciuta politicizzazione e capacità organizzativa dei gruppi criminali attivi a livello internazionale significano che le minacce interne si basano spesso su reti di attori che lavorano a livello internazionale e possono facilmente avere una dimensione di politica estera e di sicurezza.Le sfide poste da circoli intrecciati di criminalità organizzata e riciclaggio di denaro, così come la tratta di esseri umani, gli attacchi elettronici ai sistemi informatici, il terrorismo internazionale e il commercio di armi da guerra lo chiariscono a titolo di esempio (vedi Kojm, in: Goldman / Rascoff [ed.], Global Intelligence Oversight, 2016, p. 95 e seguenti; Goodman / Ischebeck-Baum, in: Dietrich / Sule [ed.], Intelligence Law and Policies in Europe, 2019, p. 1 <esp. Marginal 104 ff.>; della zona di pericolo "Cyber", vedi anche BTDrucks 18/4654, p. 40 f .; sulle zone di pericolo "terrorismo internazionale" e "proliferazione delle armi di guerra", vedi già BTDrucks 12/6853, pagg. 20, 42). Alcune di queste attività mirano a destabilizzare la comunità (cfr. Terrorismo internazionale BVerfGE 115, 320 <357>;133, 277 <333 f. Marg. 133>; 143, 101 <138 f. Marg.

125>) e può costituire una minaccia per l'ordine costituzionale, l'esistenza e la sicurezza del governo federale o degli stati federali, nonché per la vita, gli arti e la libertà. Si tratta di beni legali di eccezionale importanza costituzionale, per la protezione della quale il legislatore può considerare indispensabile un'intelligence straniera efficace e, al contempo, costituzionalmente contenuta (cfr. VerfGE 115, 320 <358>; 143, 101 <138 e seguenti. Nota marginale 124 e seguenti>).Per la protezione di cui il legislatore può considerare indispensabile un'intelligence straniera efficace e allo stesso tempo legalmente contenuta (cfr. VerfGE 115, 320 <358>; 143, 101 <138 f. Nm. 124 ff.>).Per la protezione di cui il legislatore può considerare indispensabile un'intelligence straniera efficace e allo stesso tempo legalmente contenuta (cfr. VerfGE 115, 320 <358>; 143, 101 <138 f. Nm. 124 ff.>).

164

L'ineguale accesso ai dati da parte della sorveglianza strategica oggi si pone in relazione alla situazione in cui la Corte costituzionale federale ha dovuto pronunciarsi nel 1999, il che significa che esiste anche un maggiore potenziale di rischio. Per questo motivo, l'articolo 10.1 della Legge fondamentale e i requisiti di proporzionalità che ne derivano non impediscono fondamentalmente l'inclusione di termini di ricerca personale mirati nel monitoraggio strategico e la legge può, in linea di principio, anche archiviare in misura limitata una memoria completa dei dati sul traffico e dei suoi dati fornire una valutazione senza causa.

165

(d) Infine, un aspetto importante per la giustificabilità della sorveglianza strategica delle telecomunicazioni è che le conseguenze dell'attuazione indiscriminata sono in qualche modo mitigate dal fatto che sono svolte da un'autorità che non ha poteri operativi. Alla luce delle circostanze reali, le intuizioni nei confronti delle persone all'estero di solito non possono condurre direttamente a misure di follow-up contro le persone colpite, poiché le autorità tedesche non hanno poteri sovrani. Tuttavia, ciò non rimette in discussione il fatto che la sorveglianza effettuata all'estero può anche avere gravi conseguenze per le persone colpite e che dovrebbero essere possibili anche misure di follow-up nei loro confronti, sia mediante uno scambio di dati che ai successivi valichi di frontiera.Tuttavia, poiché i dati sono raccolti da un'autorità che non ha poteri operativi propri, un ulteriore utilizzo dei dati dipende inizialmente dalla visualizzazione dei dati a distanza dalle proprie responsabilità. La loro trasmissione per uso operativo può - e deve - essere garantita da soglie di trasmissione qualificate (inferiori a 220 ff.).

166

c) Lo strumento di sorveglianza strategica, compreso l'uso di termini di ricerca personali e formali e la raccolta e la valutazione dei dati sul traffico, che a volte viene anche archiviato nella sua interezza, non è sostanzialmente incompatibile con l'articolo 10.1 della Legge fondamentale e i conseguenti requisiti di proporzionalità. Tuttavia, in quanto autorità limitata occasionale, essenzialmente solo definitiva, è un'autorità eccezionale che deve rimanere limitata alle informazioni fornite all'estero da un'autorità che non ha poteri di sicurezza operativa. È giustificato solo dal loro profilo di attività speciale. Secondo il principio di proporzionalità, anche questo deve basarsi sul progetto dettagliato.

167

2. La progettazione della raccolta e del trattamento dei dati sotto forma di monitoraggio strategico è quindi soggetta a requisiti più dettagliati, che devono tener conto del peso particolare delle

violazioni dei diritti fondamentali e della loro giustificazione specifica attraverso il profilo di compiti speciali dell'intelligence straniera.

168

a) Un obiettivo generale dei requisiti derivanti dal principio di proporzionalità è quello di progettare la sorveglianza strategica delle telecomunicazioni come uno strumento sufficientemente focalizzato, nonostante la sua portata, e quindi di limitarlo. La sorveglianza globale e generale non consente di utilizzare la Legge fondamentale a fini di informazione straniera (vedere BVerfGE 100, 313 <376>).

169

A tal fine, il legislatore deve innanzitutto specificare requisiti restrittivi per il volume di dati da esportare per i rispettivi canali di trasmissione (cfr. Löffelmann, in: Dietrich / Gärditz / Graulich / Gusy / Warg [ed.], Riforma dei servizi di intelligence tra legislazione e internazionalizzazione, 2019, pag. 33 <40>) e garantire che l'area geografica coperta dalla sorveglianza rimanga limitata. Poiché le possibilità tecniche del trattamento dei dati stanno cambiando rapidamente, non è sufficiente fare semplicemente riferimento ai limiti di capacità effettivi (cfr. Huber, ZRP 2016, p. 162 <164>; Papier, NVwZ 2016, p. 1057 <1058>; Marxsen, DÖV 2018, p. 218 <224>; Dietrich, in: Schenke / Graulich / Ruthig [ed.], Legge federale sulla sicurezza, 2a edizione 2019, § 6 BNDG Rn.11, Löffelmann, in: Dietrich / Eiffler [ed .],Manuale della legge dei servizi di intelligence, 2017, IV § 4 marg. 184). Soprattutto, tuttavia, il legislatore deve creare allegati sullo stato di diritto che strutturino la raccolta e l'elaborazione dei dati in modo più dettagliato e talvolta limitino. Questi includono, in particolare, regolamenti sull'uso delle tecnologie di filtro (b), sugli scopi di monitoraggio (c), sulla progettazione della procedura di monitoraggio (d), su un uso mirato dei termini di ricerca (e), sui limiti della memorizzazione dei dati sul traffico memorizzati (f), sui metodi valutazione dei dati (g), protezione delle relazioni di riservatezza (h) e quella dell'area centrale del progetto di vita privata (i) e specifica degli obblighi di cancellazione (j). Inoltre, vi sono requisiti di trasparenza, protezione giuridica individuale e, soprattutto, per un controllo esteso, indipendente e oggettivo-giuridico (cfr. Anche sotto V).IV § 4 marginale n. 184). Soprattutto, tuttavia, il legislatore deve creare allegati sullo stato di diritto che strutturino la raccolta e l'elaborazione dei dati in modo più dettagliato e talvolta limitino. Questi includono, in particolare, regolamenti sull'uso delle tecnologie di filtro (b), sugli scopi di monitoraggio (c), sulla progettazione della procedura di monitoraggio (d), su un uso mirato dei termini di ricerca (e), sui limiti della memorizzazione dei dati sul traffico memorizzati (f), sui metodi valutazione dei dati (g), protezione delle relazioni di riservatezza (h) e quella dell'area centrale del progetto di vita privata (i) e specifica degli obblighi di cancellazione (j). Inoltre, vi sono requisiti di trasparenza, protezione giuridica individuale e, soprattutto, per un controllo esteso, indipendente e oggettivo-giuridico (cfr. Anche sotto V).IV § 4 marginale n. 184). Soprattutto, tuttavia, il legislatore deve creare allegati sullo stato di diritto che strutturino la raccolta e l'elaborazione dei dati in modo più dettagliato e talvolta limitino. Questi includono, in particolare, regolamenti sull'uso delle tecnologie di filtro (b), sugli scopi di monitoraggio (c), sulla progettazione della procedura di monitoraggio (d), su un uso mirato dei termini di ricerca (e), sui limiti della memorizzazione dei dati sul traffico memorizzati (f), sui metodi valutazione dei dati (g), protezione delle relazioni di riservatezza (h) e quella dell'area centrale del progetto di vita privata (i) e specifica degli obblighi di cancellazione (j). Inoltre, vi sono requisiti di trasparenza, protezione giuridica individuale e, soprattutto, per un controllo esteso, indipendente e oggettivo-giuridico (cfr. Anche sotto V).Soprattutto, tuttavia, il legislatore deve creare allegati sullo stato di diritto che strutturino la raccolta e l'elaborazione dei dati in modo più dettagliato e talvolta limitino. Questi includono, in particolare, regolamenti sull'uso delle tecnologie di filtro (b), sugli scopi di monitoraggio (c), sulla progettazione della procedura di

monitoraggio (d), su un uso mirato dei termini di ricerca (e), sui limiti della memorizzazione dei dati sul traffico memorizzati (f), sui metodi valutazione dei dati (g), protezione delle relazioni di riservatezza (h) e quella dell'area centrale del progetto di vita privata (i) e specifica degli obblighi di cancellazione (j). Inoltre, vi sono requisiti di trasparenza, protezione giuridica individuale e, soprattutto, per un controllo esteso, indipendente e oggettivo-giuridico (cfr. Anche sotto V).Soprattutto, tuttavia, il legislatore deve creare allegati sullo stato di diritto che strutturino la raccolta e l'elaborazione dei dati in modo più dettagliato e talvolta limitino. Questi includono, in particolare, regolamenti sull'uso delle tecnologie di filtro (b), sugli scopi di monitoraggio (c), sulla progettazione della procedura di monitoraggio (d), su un uso mirato dei termini di ricerca (e), sui limiti della memorizzazione dei dati sul traffico memorizzati (f), sui metodi valutazione dei dati (g), protezione delle relazioni di riservatezza (h) e quella dell'area centrale del progetto di vita privata (i) e specifica degli obblighi di cancellazione (j). Inoltre, vi sono requisiti di trasparenza, protezione giuridica individuale e, soprattutto, per un controllo esteso, indipendente e oggettivo-giuridico (cfr. Anche sotto V).che strutturano e limitano parzialmente la raccolta e l'elaborazione dei dati. Questi includono, in particolare, regolamenti sull'uso delle tecnologie di filtro (b), sugli scopi di monitoraggio (c), sulla progettazione della procedura di monitoraggio (d), su un uso mirato dei termini di ricerca (e), sui limiti della memorizzazione dei dati sul traffico memorizzati (f), sui metodi valutazione dei dati (g), protezione delle relazioni di riservatezza (h) e quella dell'area centrale del progetto di vita privata (i) e specifica degli obblighi di cancellazione (j). Inoltre, vi sono requisiti di trasparenza, protezione giuridica individuale e, soprattutto, per un controllo esteso, indipendente e oggettivo-giuridico (cfr. Anche sotto V).che strutturano e limitano parzialmente la raccolta e l'elaborazione dei dati. Questi includono, in particolare, regolamenti sull'uso delle tecnologie di filtro (b), sugli scopi di monitoraggio (c), sulla progettazione della procedura di monitoraggio (d), su un uso mirato dei termini di ricerca (e), sui limiti della memorizzazione dei dati sul traffico memorizzati (f), sui metodi valutazione dei dati (g), protezione delle relazioni di riservatezza (h) e quella dell'area centrale del progetto di vita privata (i) e specifica degli obblighi di cancellazione (j). Inoltre, vi sono requisiti di trasparenza, protezione giuridica individuale e, soprattutto, per un controllo esteso, indipendente e oggettivo-giuridico (cfr. Anche sotto V).a fini di monitoraggio (c), per la progettazione del processo di monitoraggio (d), per un uso mirato dei termini di ricerca (e), per i limiti sulla memorizzazione dei dati sul traffico (f), per i metodi di valutazione dei dati (g), per la protezione delle relazioni di riservatezza (h) e quella dell'area centrale del progetto di vita privata (i) e la specifica degli obblighi di cancellazione (j). Inoltre, vi sono requisiti di trasparenza, protezione giuridica individuale e, soprattutto, per un controllo esteso, indipendente e oggettivo-giuridico (cfr. Anche sotto V).a fini di monitoraggio (c), per la progettazione del processo di monitoraggio (d), per un uso mirato dei termini di ricerca (e), per i limiti sulla memorizzazione dei dati sul traffico (f), per i metodi di valutazione dei dati (g), per la protezione delle relazioni di riservatezza (h) e quella dell'area centrale del progetto di vita privata (i) e la specifica degli obblighi di cancellazione (j). Inoltre, vi sono requisiti di trasparenza, protezione giuridica individuale e, soprattutto, per un controllo esteso, indipendente e oggettivo-giuridico (cfr. Anche sotto V).proteggere le relazioni di riservatezza (h) e quella dell'area centrale della vita privata (i) nonché la specifica degli obblighi di cancellazione (j). Inoltre, vi sono requisiti di trasparenza, protezione giuridica individuale e, soprattutto, per un controllo esteso, indipendente e oggettivo-giuridico (cfr. Anche sotto V).proteggere le relazioni di riservatezza (h) e quella dell'area centrale della vita privata (i) nonché la specifica degli obblighi di cancellazione (j). Inoltre, vi sono requisiti di trasparenza, protezione giuridica individuale e, soprattutto, per un controllo esteso, indipendente e oggettivo-giuridico (cfr. Anche sotto V).

b) Poiché la sorveglianza strategica può essere giustificata solo come strumento di intelligence straniera, la base per un'ulteriore elaborazione dei dati richiede una regolamentazione chiara standard per la separazione dei dati dalla comunicazione domestica.

171

aa) In ogni caso, è necessario un regolamento relativo alla separazione dei dati dalle telecomunicazioni, in cui tedeschi o tedeschi siano coinvolti da entrambe le parti, poiché il monitoraggio delle telecomunicazioni senza causa non è un'opzione fin dall'inizio.

172

Sulla base della separazione della comunicazione interna, il monitoraggio strategico può quindi essere effettuato con due obiettivi, vale a dire da un lato il monitoraggio della cosiddetta comunicazione "internazionale" di cui al § 5 G 10 (comunicazione nazionale-estera) e dall'altro lato il monitoraggio della pura comunicazione internazionale (comunicazione estera-estera). Entrambe le forme di sorveglianza devono ugualmente essere misurate dall'articolo 10.1 della Legge fondamentale. Tuttavia, la sorveglianza d'oltremare all'estero, per certi aspetti, è meno invadente della sorveglianza interna d'oltremare, che registra le comunicazioni con una dimensione domestica diretta e si estende quindi più in profondità nell'ordinamento giuridico nazionale. Per questo motivo, i requisiti parzialmente ridotti si applicano alla sorveglianza d'oltremare all'estero (cfr.sulla possibilità di informazioni indipendenti dal rischio per informare il governo federale al di sotto del marg. 177; sulla possibilità di selezionare i termini di ricerca solo dopo che la misura di monitoraggio è stata definita nel marg. 179 f. e per la trasmissione automatizzata di dati a servizi di intelligence esteri nell'ambito di collaborazioni al di sotto del marg. 254 ss. E 262 ss.). Se il legislatore desidera prendere in considerazione i diversi pesi degli interventi e quindi creare regolamenti diversi, deve anche prevedere che anche la comunicazione interna-straniera debba essere separata.e 262 e seguenti). Se il legislatore desidera prendere in considerazione i diversi pesi degli interventi e quindi creare regolamenti diversi, deve anche prevedere che anche la comunicazione interna-straniera debba essere separata.e 262 e seguenti). Se il legislatore desidera prendere in considerazione i diversi pesi degli interventi e quindi creare regolamenti diversi, deve anche prevedere che anche la comunicazione interna-straniera debba essere separata.

173

bb) I requisiti per la separazione della comunicazione interna e della comunicazione nazionale-estera devono essere chiaramente regolati. Per quanto tecnicamente possibile, l'uso di processi di filtro automatizzati deve garantire che i dipendenti del Servizio di intelligence federale non siano nemmeno a conoscenza di tali dati di telecomunicazione. Non è inammissibile sin dall'inizio se, nella misura in cui ciò sia tecnicamente inevitabile, tutti i dati e quindi anche i dati nazionali siano inizialmente registrati dai sistemi del Servizio di intelligence federale. Il legislatore deve quindi stabilire chiaramente che i dati provenienti da una pura comunicazione domestica e, se applicabile, da una comunicazione interna-straniera devono essere tecnicamente filtrati ed eliminati senza traccia usando tutti i mezzi disponibili.prima che abbia luogo una valutazione manuale. Il servizio è obbligato a sviluppare continuamente i metodi di filtraggio e a tenerli aggiornati con scienza e tecnologia.

174

Nella misura in cui tale filtro non può garantire completamente una separazione dei dati dovuta alla tecnologia, ciò non impedisce un ulteriore uso e valutazione dei dati pre-filtrati. A questo proposito,

tuttavia, deve essere garantito dalla legge che se i residenti tedeschi o tedeschi identificano i dati delle telecomunicazioni come parte di un'ulteriore valutazione, non devono essere utilizzati e devono essere immediatamente cancellati. Il legislatore può fare un'eccezione solo se i dati stessi mostrano un pericolo concreto imminente per la vita, l'arto o la libertà di una persona, i beni vitali vitali del pubblico in generale o l'esistenza o la sicurezza del governo federale o di un paese .Per giustificare tale autorità, i riferimenti interni ai principi generali del diritto penale non sono sufficienti (cfr. Attualmente 3.9 DV SIGINT), ma è necessario un regolamento giuridico esplicito. Potrebbe essere necessario registrare tale uso (di seguito, nm. 291) e richiedere un controllo giurisdizionale.

175

c) Inoltre, il legislatore deve definire gli scopi con sufficiente precisione e standard per i quali le telecomunicazioni sono monitorate e le conoscenze acquisite possono essere utilizzate (cfr. BVerfGE 100, 313 <372>).

176

aa) In quanto strumento educativo particolarmente intensivo di intervento, è richiesta una restrizione sostanziale a scopi sufficientemente limitati e differenziati, di cui il legislatore è responsabile. Vengono considerati gli scopi che, nei limiti della legge sulla competenza, sono finalizzati alla protezione di beni comuni di alto livello, la cui violazione comporterebbe gravi danni alla pace interna ed esterna o ai beni legali delle persone (vedere BVerfGE 100, 313 <373>) .

177

cc) Al contrario, le misure di sorveglianza dell'intelligence estera-straniera, che fin dall'inizio hanno il solo scopo di informare il governo federale e preparare le decisioni del governo, possono anche essere permesse, indipendentemente dall'attenzione al preallarme. A tal fine, il legislatore può fornire misure di sorveglianza per l'intera gamma di compiti del Servizio federale di intelligence e - anche se è già limitato a questioni di importanza di politica estera e di sicurezza - per esempio, può vincolare solo gli ordini del governo federale. Tuttavia, deve quindi garantire che un cambiamento di finalità sia escluso in linea di principio e che le conoscenze acquisite attraverso tali misure di monitoraggio - a parte casi eccezionali speciali (cfr. Marg.228) - non può essere inoltrato in altre posizioni (vedere i margini 223 e seguenti).

178

d) Al fine di perseguire gli scopi legalmente determinati, il legislatore può in linea di principio consentire una sorveglianza strategica senza causa e non deve collegarla a soglie di intervento oggettivate (margine n. 157 segg. sopra). Tuttavia, in quanto autorità con istruzioni definitive, deve vincolarle alle regole procedurali che strutturano l'allineamento ai rispettivi scopi in modo razionalizzante e quindi anche renderlo controllabile (vedi Dietrich, in: Schenke / Graulich / Ruthig [ed.], Sicherheitrechts des Bundes, 2a edizione 2019, § 6 BNDG Rn.10).

179

aa) Il punto di partenza per questo deve essere una definizione formale di misure di monitoraggio limitate. Nel senso della protezione dei dati, questo è lo scopo della misura. Come base per la loro giustificazione nei confronti del monitorato, la clausola deve specificare la misura in termini di obiettivi di conoscenza e durata. Di norma, il tipo di pericolo da chiarire e la focalizzazione

geografica del monitoraggio dovranno essere determinati. Le misure sono limitate nel tempo. Questo non impedisce un'estensione, anche ripetute.

180

Il disegno procedurale interno di tali clausole formalizzate non è prescritto costituzionalmente. I legislatori possono scegliere tra varie forme organizzative e, a seconda dell'argomento della sorveglianza, dovranno anche prendere in considerazione le riserve dei capi delle autorità o il coinvolgimento della Cancelleria federale. Nella misura in cui il legislatore limita il monitoraggio strategico ai dati relativi esclusivamente alla comunicazione internazionale, non è sempre necessario il coinvolgimento di organismi direttamente responsabili politicamente. Inoltre, i termini di ricerca non devono sempre essere determinati in anticipo quando si determina la misura (vedere l'articolo 10 Legge BVerfGE 100, 313 <373 f.>).

181

Per la determinazione della misura stessa, tuttavia, è richiesto un controllo di tipo giudiziario, conformemente alla riserva del giudice per la sorveglianza delle telecomunicazioni relativa all'individuo per ordine individuale (vedere BVerfGE 125, 260 <337 f.>; 141, 220 <312 numero marginale 235>). Fondamentalmente, questo controllo deve essere garantito in anticipo. Le eccezioni in casi urgenti non sono escluse.

182

bb) L'ulteriore processo di raccolta e valutazione dei dati deve quindi essere allineato con le finalità delle misure di monitoraggio, definite in questo modo, e successivamente rese accessibili a un controllo indipendente. Ciò vale sia per la selezione dei percorsi di trasmissione richiesti per il monitoraggio, che devono essere soggetti alla restrizione e da registrare per la valutazione, sia per la selezione dei termini di ricerca. Questo è anche il punto di riferimento per l'etichettatura e l'uso dei dati. Ciò non impedisce la creazione di regole per lo sfruttamento di reperti accidentali mediante cambiamenti di scopo all'interno dell'autorità (cfr. BVerfGE 141, 220 <326 e seguenti n. 284 e seguenti>).

183

dd) Il numero di misure di sorveglianza da stabilire in seguito non può essere limitato a poche. Sulla base della prassi corrente, che è ovviamente strutturata in modo diverso, il numero di interessi di sorveglianza o prospettive di informazione attualmente differenziate in base alla divisione del lavoro è stato stimato tra le 100 e le 200 persone all'udienza dei rappresentanti del Servizio di intelligence federale. Se queste prospettive di elaborazione sono combinate per formare misure di sorveglianza coerenti nel senso sopra menzionato, ma allo stesso tempo sufficientemente differenziate le une dalle altre, questo numero può essere leggermente ridotto. Tuttavia, è proprio lo scopo di tale strutturazione che le rispettive misure di monitoraggio abbiano un profilo chiaro e sufficientemente differenziato,che guida l'acquisizione e la valutazione dei dati in modo più dettagliato. È pertanto opportuno che il numero di misure di sorveglianza definite in questo modo sia in ogni caso significativamente superiore al numero di disposizioni di rete attualmente basate sulla prassi attuale, che attualmente ammonta a 17 (paragrafo 16 sopra).

184

Da un punto di vista costituzionale, ciò non impedisce agli accordi di rete e agli accordi di diversione basati su di essi di essere stipulati collettivamente affinché un fornitore di telecomunicazioni effettui un gran numero di diverse misure di monitoraggio. Il confronto dei dati registrati con i termini di ricerca assegnati alle varie misure può anche essere effettuato tecnicamente in un contesto e i casi di successo possono quindi essere assegnati alle rispettive misure in una fase successiva. Il modo in cui il Servizio di intelligence federale organizza tali processi tecnici non è specificato dalla costituzione.

185

e) La sorveglianza strategica ha un impatto particolare sul fatto che oggi viene effettuata principalmente utilizzando termini di ricerca formale ed è anche mirata specificamente alle singole persone. Anche questo non è escluso dalla legge costituzionale. Tuttavia, ciò richiede misure limitanti che tengano conto delle esigenze di protezione delle persone interessate in modo da soddisfare i requisiti di proporzionalità.

186

aa) Secondo la prassi attuale, la registrazione mirata delle telecomunicazioni da parte dei cittadini tedeschi deve essere esclusa. Per quanto riguarda le informazioni nazionali ed estere (vedere la Sezione 5 (2) G 10), ciò vale anche per le informazioni all'estero e all'estero. L'articolo 10.1 della Legge fondamentale protegge allo stesso modo gli stranieri e i tedeschi e giustifica la sorveglianza strategica delle telecomunicazioni di entrambi contro gravi violazioni dei diritti fondamentali. Tuttavia, ciò non rimette in discussione il fatto che tale sorveglianza abbia un peso di intervento diverso rispetto a entrambi, che devono essere presi in considerazione al momento della progettazione delle autorizzazioni di intervento previste dalla legge. La sorveglianza ha in genere un impatto maggiore sui cittadini tedeschi che sugli stranieri all'estero,perché i propri cittadini sono soggetti a un grado di accesso molto maggiore da parte delle autorità tedesche e sono quindi più facilmente esposti a misure di follow-up. Questo inizialmente si applica ai tedeschi che rimangono all'estero solo per un breve periodo. In linea di principio, tuttavia, ciò vale per tutti i cittadini tedeschi che - anche se vivono all'estero per un periodo più lungo - continuano a essere soggetti alla sovranità della Repubblica Federale Tedesca; Dipendono anche dal contatto con le autorità tedesche - anche per adempiere ai loro obblighi di identificazione legale - così come si può presumere qui che abbiano un contatto più stretto con la Germania e viaggino anche più spesso. La sorveglianza mirata delle telecomunicazioni dei cittadini tedeschi nell'ambito della sorveglianza strategica è quindi importante.che l'interferenza associata nell'Articolo 10.1 della Legge fondamentale sembrerebbe sproporzionata. Una sorveglianza mirata delle telecomunicazioni dei cittadini tedeschi deve quindi basarsi sui requisiti che si applicano alla disposizione individuale di una sorveglianza delle telecomunicazioni (cfr. Requisiti BVerfGE 141, 220 <268 e seguenti. Margine 103 e seguenti; 309 e seguenti. Margine 228 e seguenti .>).

187

bb) Inoltre, il legislatore deve definire le possibili ragioni e punti di vista, in base ai quali le misure strategiche di sorveglianza possono essere rivolte a persone specifiche, come base per una strutturazione mirata del processo di sorveglianza. Ad esempio, può provvedere al monitoraggio di persone che sono considerate possibili fonti di pericolo, come mediatore di notizie o come informatori altrimenti più qualificati e può stabilire regole di preferenza in base alle quali il monitoraggio mirato di persone completamente non coinvolte è solo subordinato. Anche a questo proposito, tuttavia, non deve richiedere la presenza di soglie di intervento oggettivate, ma può farlo

specificando gli scopi per i quali le persone possono essere monitorate in modo specifico,e, a sua volta, soddisfano solo i requisiti finali.

188

A tale proposito, il legislatore deve prevedere un proprio meccanismo di protezione per le persone che sono possibili cause di pericoli o che sono nell'interesse diretto del servizio di intelligence in vista delle misure di follow-up da adottare. La sorveglianza ha un'intensità speciale nei loro confronti e vi è una maggiore probabilità di conseguenze stressanti. All'udienza, il servizio di intelligence federale ha dichiarato che circa il cinque percento dei termini di ricerca sono attualmente rivolti a tali persone. Nella misura in cui le misure di sorveglianza sono dirette contro determinate persone in questo modo, per determinarle è necessario un controllo ex ante simile a un tribunale. Questo deve controllarese la sorveglianza personale mirata a perseguire l'obiettivo della sorveglianza soddisfa i requisiti di proporzionalità.

189

cc) Per inciso, il limite della possibile autorizzazione per una sorveglianza occasionale è dove l'uso di un termine di ricerca personale porta fin dall'inizio con una sicurezza e un effetto quasi comparabili come un accordo individuale per una sorveglianza individualizzata del traffico delle telecomunicazioni. I legislatori devono garantire che i requisiti pertinenti (vedere BVerfGE 141, 220 <268 e seguenti Marginal 103 e seguenti; 309 e seguenti Marginali e seguenti 228)>) siano quindi soddisfatti e non compromessi dal monitoraggio strategico.

190

dd) Il legislatore può rinunciare alle disposizioni e alle restrizioni di cui sopra (solo marginali 187 e seguenti) se le misure di sorveglianza sono intese e mirate esclusivamente a informazioni politiche del governo federale e un trasferimento di conoscenze ad altri organismi è principalmente escluso (sopra il marginale no 177).

191

f) L'autorizzazione per il monitoraggio strategico richiede anche restrizioni legali nella misura in cui apre una memorizzazione globale dei dati sul traffico. Il legislatore deve garantire che i flussi di dati registrati per questo rimangano sostanzialmente limitati e che non si debba superare un periodo di conservazione massimo di sei mesi (cfr. Anche BVerfGE 125, 260 <322>).

192

g) Per le singole fasi della valutazione dei dati registrati, è sufficiente che il legislatore specifichi le basi essenziali e altrimenti rinunci alla struttura più dettagliata al Servizio di intelligence federale per la regolamentazione di diritto interno, che ovviamente deve essere soggetta a controllo legale oggettivo indipendente (vedi margine n. 272 ss. sotto) .). Il quadro giuridico prevede che i dati raccolti vengano valutati immediatamente (vedere BVerfGE 100, 313 <385 f.>; 125, 260 <332>; vedere anche la disposizione corrispondente nella Sezione 6 (1) frase 1 G 10 e il materiale legislativo associato BTDrucks 14/5655, p. 13), la validità del principio di proporzionalità nella scelta dei termini di ricerca - come già previsto dalla legge nel regolamento del servizio - ,Regolamenti sull'uso di metodi di valutazione dei dati ad alta intensità di intervento, in particolare forme complesse di confronto dei dati (cfr. Anche la necessità speciale di regolamenti di valutazione per il monitoraggio strategico anche EGMR, Big Brother Watch e altri c. Regno Unito,

sentenza del 13 settembre 2018, n. 58170 / 13 e altri, §§ 346 f.) Oltre all'osservanza del divieto costituzionale di discriminazione (cfr. Per questo requisito BVerfGE 115, 320 <348>; 133, 277 <359 f. Margine 189>; sulla situazione giuridica svedese a tale riguardo EGMR, Centrum för Rättvisa v. Svezia, sentenza del 19 giugno 2018, n. 35252/08, § 29). Se necessario, anche l'uso di algoritmi deve essere regolamentato, in particolare garantendo la loro tracciabilità di base in vista di un controllo indipendente.in particolare forme complesse di confronto dei dati (cfr. anche EGMR, Big Brother Watch e altri c. Regno Unito, sentenza del 13 settembre 2018, n. 58170/13 e altri, §§ 346 f. sulla particolare necessità di regolamenti di valutazione per il monitoraggio strategico) così come l'osservanza dei divieti costituzionali di discriminazione (cfr. su questo requisito BVerfGE 115, 320 <348>; 133, 277 <359 f. margine n. 188>; sulla situazione giuridica svedese al riguardo EGMR, Centrum för Rättvisa v. Svezia, sentenza del 19 giugno 2018, n. 35252/08, § 29). Se necessario, anche l'uso di algoritmi deve essere regolamentato, in particolare garantendo la loro tracciabilità di base in vista di un controllo indipendente.in particolare forme complesse di confronto dei dati (cfr. anche EGMR, Big Brother Watch e altri c. Regno Unito, sentenza del 13 settembre 2018, n. 58170/13 e altri, §§ 346 f. sulla particolare necessità di regolamenti di valutazione per il monitoraggio strategico) così come l'osservanza dei divieti costituzionali di discriminazione (cfr. su questo requisito BVerfGE 115, 320 <348>; 133, 277 <359 f. margine n. 188>; sulla situazione giuridica svedese al riguardo EGMR, Centrum för Rättvisa v. Svezia, sentenza del 19 giugno 2018, n. 35252/08, § 29). Se necessario, anche l'uso di algoritmi deve essere regolamentato, in particolare garantendo la loro tracciabilità di base in vista di un controllo indipendente.EGMR, Big Brother Watch e altri v. Sulla necessità speciale di regolamenti di valutazione per il monitoraggio strategico. Regno Unito, sentenza del 13 settembre 2018, n. 58170/13 e altri, §§ 346 f.) Oltre all'osservanza del divieto costituzionale di discriminazione (cfr. Su questo requisito BVerfGE 115, 320 <348>; 133, 277 <359 f. Punto 189>; sulla situazione giuridica svedese al riguardo EGMR, Centrum för Rättvisa contro Svezia, sentenza del 19 giugno 2018, n. 35252/08, § 29). Se necessario, anche l'uso di algoritmi deve essere regolamentato, in particolare garantendo la loro tracciabilità di base in vista di un controllo indipendente.EGMR, Big Brother Watch e altri v. Sulla necessità speciale di regolamenti di valutazione per il monitoraggio strategico. Regno Unito, sentenza del 13 settembre 2018, n. 58170/13 e altri, §§ 346 f.) Oltre all'osservanza del divieto costituzionale di discriminazione (cfr. Su questo requisito BVerfGE 115, 320 <348>; 133, 277 <359 f. Punto 189>; sulla situazione giuridica svedese al riguardo EGMR, Centrum för Rättvisa contro Svezia, sentenza del 19 giugno 2018, n. 35252/08, § 29). Se necessario, anche l'uso di algoritmi deve essere regolamentato, in particolare garantendo la loro tracciabilità di base in vista di un controllo indipendente.su questo requisito BVerfGE 115, 320 <348>; 133, 277 <359 f. Marg. 189>; sulla situazione giuridica svedese per quanto riguarda l'EGMR, Centrum för Rättvisa v. Svezia, sentenza del 19 giugno 2018, n. 35252/08, § 29). Se necessario, anche l'uso di algoritmi deve essere regolamentato, in particolare garantendo la loro tracciabilità di base in vista di un controllo indipendente.su questo requisito BVerfGE 115, 320 <348>; 133, 277 <359 f. Marg. 189>; sulla situazione giuridica svedese per quanto riguarda l'EGMR, Centrum för Rättvisa v. Svezia, sentenza del 19 giugno 2018, n. 35252/08, § 29). Se necessario, anche l'uso di algoritmi deve essere regolamentato, in particolare garantendo la loro tracciabilità di base in vista di un controllo indipendente.

193

h) Requisiti speciali devono essere posti sulla protezione delle relazioni di riservatezza, in particolare tra giornalisti e loro informatori o avvocati e loro clienti. Questa protezione deriva dall'articolo 10.1 della Legge fondamentale e dai requisiti di proporzionalità da essa derivati. Corrisponde a una crescente necessità di protezione in tali relazioni, che possono esistere su entrambi i lati della comunicazione. Per i gruppi professionali interessati, la protezione è garantita al contempo dall'articolo 5, paragrafo 1, frase 2 della legge di base o dai diritti di base che altrimenti

garantiscono la loro protezione - nella misura in cui si applica alla protezione del personale straniero in termini di protezione personale.

194

aa) Per quanto riguarda i gruppi professionali e i gruppi di persone le cui relazioni di comunicazione richiedono una protezione speciale della riservatezza, il loro monitoraggio mirato deve essere innanzitutto limitato. L'uso di termini di ricerca che portano a una registrazione mirata delle connessioni di telecomunicazione di tali persone non può essere giustificato dal fatto che può essere utilizzato per ottenere informazioni potenzialmente rilevanti per il servizio di intelligence. L'attività giornalistica non giustifica l'esposizione delle persone a un rischio di sorveglianza più elevato rispetto ad altre entità per i diritti fondamentali e il fatto di renderle oggetto di raccolta di informazioni per perseguire interessi di sicurezza a causa dei loro contatti e ricerche (vedere BVerfGE 107, 299 <336>). Lo stesso vale per gli avvocati.Piuttosto, il loro monitoraggio mirato come mediatore di notizie deve essere collegato a soglie di intervento qualificate come parte del monitoraggio strategico. In base a ciò, si deve garantire che l'intrusione nei rapporti di riservatezza sia consentita solo per indagare su pericoli gravi e reati particolarmente gravi o per sequestrare alcuni criminali pericolosi. Ciò richiede una conoscenza affidabile. Per il resto, il monitoraggio e la valutazione sono consentiti solo se l'interesse pubblico per le informazioni supera l'interesse delle persone interessate a proteggere la riservatezza nei singoli casi (vedere BVerfGE 129, 208 <258 e seguenti>; 141, 220 < 318 s. Marginale 255 ss.>). Il legislatore dovrà considerarese e in che misura è necessario differenziare ulteriormente tra le diverse relazioni di riservatezza (vedere § 160a StPO; vedere BVerfGE 129, 208 <259 f.>). In ogni caso, la tua protezione deve essere sempre salvaguardata da un controllo ex ante di tipo giudiziario.

195

Nella misura in cui la registrazione di relazioni di riservatezza particolarmente meritevoli di protezione viene notata solo nel corso della valutazione, è anche necessario verificare i requisiti e, se necessario, quindi valutare se la comunicazione corrispondente può essere valutata e utilizzata (Löffelmann applicabile, in: Dietrich / Gärditz / Graulich / Gusy / Warg [ed.], Riforma dei servizi di intelligence tra legalizzazione e internazionalizzazione, 2019, p. 33 <43 con nota 41>; contrariamente a Gärditz, DVBl 2017, p. 525 <528>). Anche in questo caso dipende dal fatto che si debba acquisire la conoscenza di rischi gravi ed emergenti e l'interesse pubblico in questo avrà la precedenza sulla protezione della riservatezza in conformità con una considerazione nei singoli casi.Questa decisione richiede anche un controllo giudiziario.

196

bb) Per la protezione dei gruppi professionali e delle loro attività nel contesto delle informazioni straniere, il legislatore può tener conto delle varie circostanze in cui la stampa o gli avvocati operano in altri paesi. Può quindi limitare la protezione a persone e situazioni che sono effettivamente meritevoli di protezione, vale a dire la cui attività è caratterizzata da libertà e indipendenza che giustificano la speciale protezione dei diritti fondamentali di queste istituzioni (vedi Dietrich, in: Schenke / Graulich / Ruthig [Ed.], Federal Security Law, 2nd edition 2019, § 6 BNDG Rn. 10 aE). A questo proposito, i fattori decisivi sono le decisioni di valore risultanti dai diritti fondamentali della Legge fondamentale, che a loro volta sono incorporati nelle garanzie internazionali dei diritti umani (cfr. Art. 1 cpv. 2 GG).Le incertezze devono essere contrastate sulla base di valutazioni informate.

197

cc) Spetta al legislatore determinare se e in quale misura altre relazioni di riservatezza possano essere soddisfatte mediante misure di protezione.

198

dd) Nella misura in cui le misure di sorveglianza, indipendentemente dal loro scopo giustificativo per l'individuazione precoce dei pericoli, sono esclusivamente destinate e mirate a servire le informazioni politiche del governo federale e un trasferimento delle conoscenze ad altri organismi è sostanzialmente escluso (punto 177 supra), la protezione di Le relazioni di riservatezza vengono revocate nella misura in cui ciò sia necessario.

199

i) Ulteriori requisiti derivano dall'articolo 10 capoverso 1 GG in relazione all'articolo 1 capoverso 1 GG per proteggere l'area centrale della vita privata.

200

aa) La protezione dell'area centrale della vita privata garantisce all'individuo un'area di privacy personale e garantisce una protezione dei diritti umani dei diritti fondamentali contro la sorveglianza che non è disponibile allo stato. Persino gli interessi in sospeso del grande pubblico non possono giustificare interferenze in questa area assolutamente protetta della vita privata (vedere BVerfGE 109, 279 <313>; 141, 220 <276 paragrafo 120>; stRspr). Ciò vale anche per i servizi di intelligence (vedi BVerfGE 120, 274 <335 ss.>) E anche per le misure di sorveglianza all'estero.

201

Lo sviluppo della personalità nell'area centrale della vita privata include l'opportunità di esprimere processi interni, considerazioni ed esperienze di natura molto personale. Protetta è in particolare la comunicazione non pubblica con persone di fiducia personale, che si basa sul presupposto giustificato che non sarà monitorata. Tali conversazioni non perdono il loro carattere di persona nel suo insieme perché combinano il più personale e quotidiano (vedi BVerfGE 141, 220 <276 f. Marginale 121; 279 marginale 128; 314 f. Marginale 243>; stRspr).

202

Al contrario, la discussione e la pianificazione dei crimini non fanno parte dell'area centrale della vita privata, anche se coinvolgono anche questioni altamente personali. Ciò non significa che l'area centrale sia soggetta a un compromesso generale per quanto riguarda gli interessi di pubblica sicurezza. Una conversazione personale non rientra nell'area centrale della progettazione della vita privata perché la conoscenza dei suoi contenuti può fornire informazioni utili per l'indagine sui crimini o la prevenzione dei pericoli. Se le dichiarazioni esprimono solo impressioni e sentimenti interiori senza contenere alcuna prova di specifici reati penali, non ottengono una connessione comunitaria semplicemente essendo in grado di scoprire le cause o le motivazioni del comportamento criminale.Nonostante il fatto che sia stato commesso un reato, le situazioni in cui si presume che gli individui possano ammettere azioni illecite o agire di conseguenza, come colloqui confessionali o conversazioni riservate con uno psicoterapeuta o un avvocato difensore, possono essere soggette alla privacy personale (vedere BVerfGE 141, 220 per maggiori dettagli 276 f. Marginale 121 f.>; StRspr).

203

bb) Il legislatore deve garantire la protezione dell'area centrale della vita privata attraverso i propri regolamenti.

204

A questo proposito, è assolutamente necessario escludere innanzitutto di rendere l'area centrale l'obiettivo delle indagini governative e di utilizzare le informazioni a tale riguardo in qualsiasi modo o di usarle come base per ulteriori indagini. Ciò vale anche per il monitoraggio strategico. La comprensione dell'area centrale, in accordo con la comprensione presentata, non deve limitarsi a situazioni in cui "solo" domande altamente personali sono oggetto.

205

Inoltre, la protezione dell'area centrale deve sempre essere presa in considerazione a due livelli: a livello di raccolta dei dati e a livello di valutazione dei dati. A questo proposito, tuttavia, i requisiti per la tutela legale di questa protezione differiscono a seconda del tipo di misura di sorveglianza in questione (vedi BVerfGE 141, 220 <279 marginale n. 127>).

206

In base a ciò, per la raccolta dei dati e l'uso di termini di ricerca per il monitoraggio strategico non sono necessarie ulteriori misure precauzionali legali oltre al divieto di copertura mirata dell'area centrale. Dato che in genere non è possibile riconoscere dai termini di ricerca in quanto tali che la comunicazione rilevante per l'area centrale viene registrata con una probabilità significativa, non sono richiesti regolamenti specifici volti a separare in anticipo i selettori pertinenti all'area centrale. Ciò non influisce sul fatto che, nella misura in cui l'uso dei termini di ricerca evidenzia chiaramente una significativa probabilità di catturare le comunicazioni relative all'area centrale, ciò deve, se possibile, essere escluso dalla raccolta in anticipo in termini di tecnologia dell'informazione (vedi BVerfGE 141, 220 <306 ss. Margine n. 210 ss. >).

207

Al contrario, tuttavia, a livello di valutazione manuale dei dati, la legge deve garantire che ulteriori valutazioni debbano essere immediatamente interrotte se risulta evidente che la sorveglianza sta entrando nell'area centrale della progettazione della vita personale; Anche in caso di dubbi, la loro continuazione - fatti salvi i regolamenti per i casi urgenti (vedi BVerfGE 141, 220 <280 margine n. 129>) - può essere consentita solo sotto forma di documenti che devono essere visualizzati da un organismo indipendente prima della loro valutazione (vedi BVerfGE 141, 220 <279 f.N. 129>; vedere anche la sezione 3a frasi da 2 a 11 G 10). Deve essere chiaro che le conoscenze provenienti dall'area della vita altamente personale non devono essere utilizzate e devono essere immediatamente cancellate; questo deve essere registrato e i registri di cancellazione devono essere conservati per un periodo sufficientemente lungo per garantire il controllo della protezione dei dati (cfr. BVerfGE 141, 220 <280 marginale n. 129>; vedere anche il marginale n. 289 e seguenti).

208

j) I requisiti di proporzionalità per le misure di sorveglianza comprendono anche la specifica degli obblighi di cancellazione. Sono utilizzati per garantire che l'uso dei dati personali sia limitato alle finalità che giustificano il trattamento dei dati e non è più possibile dopo che è stato completato (vedere BVerfGE 65, 1 <46>; 133, 277 <366 marginale 206>; 141, 220 <285 f. Marginale 144>; stRspr).

209

Per le misure di sorveglianza che - come nella fattispecie - funzionano acquisendo grandi quantità di dati, ma a cui è consentito loro solo un accesso parziale, i regolamenti di cancellazione devono garantire che i dati inizialmente registrati, che sono costituzionalmente ritirati dalla revisione relativa al contenuto, siano immediatamente separati, nonché senza traccia e finale essere cancellato. Se la valutazione dei dati avviene quindi in più fasi, in cui la quantità di dati è sempre più limitata, sono richiesti standard chiari alla norma, che prevedono una rapida valutazione e quindi la cancellazione immediata dei dati separati ad ogni livello (vedere BVerfGE 100, 313 < 385; 400>). Nella misura in cui le informazioni sono classificate come pertinenti e dovrebbero essere conservate più a lungo in vista di un ulteriore utilizzo,per questo devono essere creati regolamenti adeguati. In questo caso, gli obblighi di ispezione devono essere forniti a intervalli sufficientemente stretti (cfr., Ad esempio, Sezione 6 (1) G 10; vedere BVerfGE 100, 313 <400>), che impediscono l'archiviazione dei dati senza giustificazione.

210

Le fasi centrali della cancellazione dei dati devono essere registrate nella misura in cui ciò ha senso ed è necessario per un controllo indipendente; i registri di eliminazione devono essere conservati per un periodo di tempo sufficiente per consentire un controllo efficace (vedere BVerfGE 141, 220 <302 f. marginale 205>; vedere anche marginale 291 di seguito).

III.

211

I dati personali provenienti dalla sorveglianza strategica possono essere trasmessi ad altre posizioni solo se la trasmissione è collegata alla protezione degli interessi legali e delle soglie di intervento che tengono conto del peso dell'intervento della sorveglianza strategica attraverso una base giuridica chiara e sufficientemente definita. In base a ciò, i trasferimenti sono giustificati solo per la protezione di attività legali particolarmente importanti e richiedono una specifica situazione di rischio o un sospetto sufficientemente specificato come soglia di trasmissione. Lo stesso vale per le segnalazioni al governo federale nella misura in cui sono utilizzate solo per informazioni politiche e per preparare le decisioni del governo.

212

1. La trasmissione di dati personali, con la quale un'autorità rende i dati raccolti da essa accessibili a un altro ente, costituisce la propria interferenza con i diritti fondamentali (cfr. BVerfGE 100, 313 <367>; 141, 220 <334 marg. 305>; stRspr). Questo deve essere misurato rispetto al diritto fondamentale che è stato interferito nella raccolta dei dati originali (cfr. VerfGE 100, 313 <367>; 141, 220 <334 Rn. 305>; stRspr).

213

2. Come nuova interferenza con i diritti fondamentali, i trasferimenti devono avere una propria base giuridica chiara e sufficientemente definita (cfr. BVerfGE 65, 1 <46>; 100, 313 <389>; stRspr).

214

La natura intrusiva della trasmissione dei dati esclude - sulla base dei dati in questione da misure di sorveglianza particolarmente intense a livello di intervento - la trasmissione o lo scambio di dati senza basi giuridiche specifiche, che a tale riguardo hanno anche una funzione di avvertimento e chiarimento.

215

La chiarezza degli standard pone limiti all'uso delle catene di riferimento legali. Non manca una chiara base giuridica semplicemente perché uno standard fa riferimento a un altro standard. Tuttavia, i riferimenti devono rimanere limitati, non devono perdere la loro chiarezza facendo riferimento a norme che affrontano tensioni diverse e non devono comportare eccessive difficoltà di applicazione nella pratica. Pertanto, confuse cascate di riferimenti non sono compatibili con i requisiti dei diritti fondamentali (vedere BVerfGE 110, 33 <57 f.; 61 ff.>).

216

3.Materialmente, sia le autorizzazioni legali per la trasmissione dei dati che le misure di trasmissione nei singoli casi devono soddisfare i requisiti di proporzionalità (vedere BVerfGE 65, 1 <45 f.>; 100, 313 <390 ff.>; 141, 220 <327 marg. 286>). La trasmissione deve essere idonea e necessaria per raggiungere uno scopo legittimo. Secondo una costante giurisprudenza, il punto di partenza per determinare la proporzionalità in senso stretto è il peso del cambiamento di scopo nella trasmissione rispetto allo scopo della raccolta dei dati e, sulla base di ciò, il criterio della raccolta ipotetica dei dati. Successivamente, dipende dal fatto che i dati pertinenti possano anche essere compilati per lo scopo modificato utilizzando mezzi comparabili e gravi secondo gli standard costituzionali (cfr. BVerfGE 141,220 <327 ss. Marg. 287 ss.>).

217

A questo proposito, tuttavia, devono essere prese in considerazione caratteristiche speciali per la presente costellazione. Mentre le autorità normalmente raccolgono dati per scopi operativi propri specifici e poi li trasferiscono a un'altra autorità per un nuovo scopo, il Servizio di intelligence federale non raccoglie i propri dati per i propri scopi operativi, ma fin dall'inizio con il solo scopo di filtrarli ed elaborarli Informazioni pertinenti - da trasmettere al governo federale e, se necessario, ad altre agenzie (cfr. Sezione 1 (2) BNDG). I poteri di raccolta dei dati si caratterizzano anche nel caso in esame in quanto non sono legati a soglie di intervento oggettivate, ma sono essenzialmente dati solo in maniera definitiva.

218

Per questa costellazione in particolare, è di particolare importanza osservare requisiti di trasmissione sostanziali. Se la raccolta di dati per le informazioni all'estero non richiede di per sé soglie di intervento verificabili e dovrebbe quindi consentire di identificare minacce e pericoli con largo anticipo rispetto ai pericoli concreti e di cercarli in modo proattivo, ciò richiede la legge costituzionale in cambio che le soglie di intervento corrispondenti almeno per deve essere applicata la trasmissione delle conoscenze acquisite (cfr. Gärditz, DVBl 2017, p. 525 <526>). Lo scopo della raccolta dei dati e lo scopo della trasmissione dei dati si fondono in questo senso: al servizio di intelligence sono stati dati ampi poteri di chiarimento,in modo che possa filtrare le informazioni importanti prima delle attività operative basate su una grande quantità di dati in gran parte non strutturati. Uno degli scopi principali della raccolta dei dati è la differenziazione tra dati pertinenti e irrilevanti, che determina quali informazioni sono portate all'attenzione del governo e, se necessario, altri organismi che sono autorizzati ad agire. A questo proposito, tuttavia, a livello degli standard di

trasmissione si deve garantire che le conoscenze acquisite a causa di poteri essenzialmente non motivati siano accessibili per ulteriori elaborazioni se la raccolta dei dati sarebbe giustificata ai fini della trasmissione in conformità con i requisiti generali dello Stato di diritto.Uno degli scopi principali della raccolta dei dati è la differenziazione tra dati pertinenti e irrilevanti, che determina quali informazioni sono portate all'attenzione del governo e, se necessario, altri organismi che sono autorizzati ad agire. A questo proposito, tuttavia, a livello degli standard di trasmissione si deve garantire che le conoscenze acquisite a causa di poteri essenzialmente non motivati siano accessibili per ulteriori elaborazioni se la raccolta dei dati sarebbe giustificata ai fini della trasmissione in conformità con i requisiti generali dello Stato di diritto.Uno degli scopi principali della raccolta dei dati è la differenziazione tra dati pertinenti e irrilevanti, che determina quali informazioni sono portate all'attenzione del governo e, se necessario, altri organismi che sono autorizzati ad agire. A questo proposito, tuttavia, a livello degli standard di trasmissione si deve garantire che le conoscenze acquisite a causa di poteri essenzialmente non motivati siano accessibili per ulteriori elaborazioni se la raccolta dei dati sarebbe giustificata ai fini della trasmissione in conformità con i requisiti generali dello Stato di diritto.è uno scopo essenziale della raccolta dei dati. A questo proposito, tuttavia, a livello degli standard di trasmissione si deve garantire che le conoscenze acquisite a causa di poteri essenzialmente non motivati siano accessibili per ulteriori elaborazioni se la raccolta dei dati sarebbe giustificata ai fini della trasmissione in conformità con i requisiti generali dello Stato di diritto.è uno scopo essenziale della raccolta dei dati. A questo proposito, tuttavia, a livello degli standard di trasmissione si deve garantire che le conoscenze acquisite a causa di poteri essenzialmente non motivati siano accessibili per ulteriori elaborazioni se la raccolta dei dati sarebbe giustificata ai fini della trasmissione in conformità con i requisiti generali dello Stato di diritto.

219

In base a ciò, la costituzionalità della trasmissione dipende anche dal fatto che i dati debbano essere raccolti secondo gli standard costituzionali ai fini della trasmissione con mezzi comparabili ad alta intensità di intervento (vedere BVerfGE 141, 220 <328 paragrafo 288>). Poiché le autorità di sicurezza non sono autorizzate a disporre di uno strumento di vasta portata come la sorveglianza domestica delle telecomunicazioni fin dall'inizio, a meno che l'unica domanda al governo federale sia la segnalazione (nm. 223 e seguenti), i requisiti costituzionali che altrimenti si applicano per altre misure di intervento particolarmente gravi come la sorveglianza degli alloggi o la ricerca online (cfr. BVerfGE 141, 220 <271 marginale 110; 273 f. marginale 115 f.; 327 ff. marginale 287 ff.>).Ciò corrisponde al requisito di un interesse pubblico eccezionale e di soglie di trasmissione sufficientemente concrete e qualificate, come richiesto anche dalla Corte costituzionale federale per la trasmissione di informazioni di intelligence alle autorità operative nella decisione sulla legge antiterrorismo (cfr. VerfGE 133, 277 <329 para 123>) e concretizza questo.

220

4. In base a ciò, i requisiti devono essere posti sia sulla protezione degli interessi legali sia sulle soglie di intervento, qui sotto forma di soglie di trasmissione. È necessario operare una distinzione tra trasferimenti per motivi di sicurezza e azioni penali (vedere BVerfGE 100, 313 <394>; 141, 220 <270 f. Marginal 107 f.>).

221

Per quanto riguarda la protezione legale delle merci, una trasmissione a fini di sicurezza è consentita solo per la protezione di merci legali particolarmente importanti (vedere BVerfGE 125, 260 <329 f.>; 133, 277 <365 marg. 203>; 141, 220 <270 marginale 108>). Nella misura in cui la

legge prevede un cambiamento di scopo, la trasmissione non deve mirare a proteggere la stessa risorsa legale dell'ordine di sorveglianza dell'intelligence. Fondamentalmente, ciò dovrebbe basarsi direttamente sui beni legali stessi, non su cataloghi di reati; in ogni caso, un riferimento a reati non deve riguardare le situazioni in cui la soglia di responsabilità penale viene spostata nel periodo precedente ai pericoli attraverso la penalizzazione di atti preparatori o semplici minacce ai diritti legali (vedere BVerfGE 125, 260 <329 f.>).Una trasmissione a fini di contrasto, d'altro canto, deve essere limitata dall'obbligo di ponderare i reati in questione. Secondo questi criteri, è giustificato solo per il perseguimento di reati particolarmente gravi. Di norma, questi dovranno essere specificati più dettagliatamente nel catalogo dei reati.

222

Per quanto riguarda le soglie di trasmissione, è necessaria una situazione di pericolo sufficientemente concreta e prevedibile per la difesa dal pericolo. Secondo il tradizionale modello di sicurezza, il legislatore non deve effettuare trasferimenti dipendenti dalla difesa contro un pericolo concreto, imminente o attuale. Tuttavia, deve essere richiesto un rischio sufficientemente specifico nel senso che vi sono almeno indicazioni concrete che insorga un pericolo specifico per le merci protette (cfr. BVerfGE 141, 220 <271 ss. Numero marginale 111 ss.>). Nella misura in cui vengono trasmessi dati sull'azione penale, sono necessari fatti concreti sufficienti per giustificare il sospetto di un crimine particolarmente grave. Per questo, le semplici indicazioni non sono sufficienti, poiché sono sufficiential fine di avviare indagini generali (vedi Sezione 152 (2) StPO), sono necessari alcuni fatti per sospettare tali crimini (vedi BVerfGE 125, 260 <328 f.>), come la sorveglianza degli alloggi ai sensi della Sezione 100c StPO potrebbe giustificare. A questo proposito, ci devono essere circostanze concrete e in una certa misura condensate come base fattuale per il sospetto (cfr. Bruns, in: Karlsruher Comment zur StPO, 8a edizione 2019, § 100c Rn. 10 mwN).Commento di Karlsruhe alla StPO, 8a edizione 2019, § 100c marginale n. 10 mwN).Commento di Karlsruhe alla StPO, 8a edizione 2019, § 100c marginale n. 10 mwN).

223

5. È diverso se la trasmissione delle conoscenze dalla sorveglianza strategica al governo federale è solo in questione nella sua funzione di governo. Quando si tratta di informare il governo federale in merito all'esercizio della propria responsabilità in materia di politica estera e di sicurezza e di inoltrarlo ad altri organismi, i requisiti per la protezione giuridica qualificata delle merci o per le soglie di trasmissione non sono costituzionalmente richiesti.

224

a) Tali requisiti aggiuntivi non sono necessari in questo caso, poiché le informazioni fornite al governo federale su questioni di rilevanza politica estera e di sicurezza devono soddisfare lo scopo primario dell'intelligence straniera, in cui deve essere riconosciuto un interesse pubblico prevalente, indipendentemente dalla specifica situazione di rischio.

225

Soprattutto, l'interferenza con i diritti fondamentali nei confronti delle persone monitorate è generalmente molto meno importante delle semplici informazioni politiche fornite al governo federale. Nella misura in cui non vi è alcun dubbio sulle persone che svolgono funzioni politiche statali dirette all'estero, contro le quali l'interesse pubblico può fondamentalmente giustificare la sorveglianza, tali rapporti spesso non saranno pertinenti ai dati personali, pertanto è possibile separarli e rimuoverli. Tuttavia, anche se è necessario includere informazioni personali nei rapporti,

tali rapporti sono sostanzialmente diversi dalla trasmissione di conoscenze sugli individui alle autorità nazionali,che, a loro volta, direttamente o indirettamente, hanno i propri poteri di agire e possono anche essere in grado di usarli contro le persone colpite. Ciò è particolarmente vero se paragonato alla trasmissione a corpi estranei. Se utilizzato come informazione di base dal governo federale o come base per la preparazione delle decisioni del governo, l'interesse per le persone colpite in modo specifico svanisce, in modo che la trasmissione possa essere giustificata indipendentemente dal rispetto delle soglie di trasmissione specifiche.Se utilizzato come informazione di base dal governo federale o come base per la preparazione delle decisioni del governo, l'interesse per le persone colpite in modo specifico svanisce, in modo che la trasmissione possa essere giustificata indipendentemente dal rispetto delle soglie di trasmissione specifiche.Se utilizzato come informazione di base dal governo federale o come base per la preparazione delle decisioni del governo, l'interesse per le persone colpite in modo specifico svanisce, in modo che la trasmissione possa essere giustificata indipendentemente dal rispetto delle soglie di trasmissione specifiche.

226

Tuttavia, tali rapporti al governo federale servono solo per informazioni politiche a livello governativo. Nella misura in cui le informazioni sono rese disponibili indipendentemente da una soglia di trasmissione, il loro uso è quindi limitato alle decisioni dello stesso governo federale in materia di politica estera e di sicurezza. Può usarlo - anche in comunicazione con i governi stranieri e le organizzazioni internazionali - per svolgere i suoi compiti, a meno che non venga trasmesso alle autorità subordinate in Germania e all'estero per altri scopi, in particolare anche operativi. Lo stesso vale per la comunicazione tra il governo federale e i governi degli stati federali.

227

b) Nella misura in cui le informazioni provengono da misure di sorveglianza basate sugli scopi della rilevazione precoce dei pericoli e quindi - come in pratica fino ad ora di norma - sono destinate a fornire sia le informazioni generali del governo federale sia la tempestiva chiarificazione dei pericoli, è possibile ottenere i risultati corrispondenti può essere utilizzato oltre gli scopi del lavoro governativo. Se le informazioni in questo senso devono essere inoltrate tramite il governo federale o i governi statali ad altri organismi operativi - come in particolare le autorità di sicurezza o l'amministrazione nazionale - ciò richiede, come la trasmissione diretta dei dati ad altri organismi, autorizzazioni legali di trasmissione,che soddisfano i requisiti di protezione legale qualificata e la presenza di soglie di intervento.

228

c) Anche sulla base dei propri regolamenti di trasmissione, in linea di principio è escluso l'inoltro in altri luoghi se i dati provengono da misure di sorveglianza che non erano giustificate sin dall'inizio dagli obiettivi della rilevazione precoce del pericolo e indipendentemente dagli interessi di informazione relativi al pericolo esclusivamente per l'informazione politica del governo federale - è stato effettuato il governo (paragrafi 177 e 226 sopra). In questi casi, non è possibile trasferire la conoscenza ad altri organismi mediante un regolare cambio di finalità. Il legislatore può fornire un'eccezione solo se i dati stessi rappresentano un pericolo imminente per la vita, l'arto o la libertà di una persona,per beni vitali del grande pubblico o per l'esistenza o la sicurezza del governo federale o di un paese (vedi margine 174 sopra).

229

6. Poiché la trasmissione di dati ad altri organismi giustifica la propria ingerenza con i diritti fondamentali, presuppone - al contrario la trasmissione di dati personali da altre autorità al Servizio di intelligence federale - una decisione formale, in cui devono essere verificati i rispettivi requisiti legali di trasmissione. Dati i suoi ampi poteri, il Servizio di intelligence federale ha una responsabilità speciale. Proprio come, da un lato, ha poteri particolarmente ampi che consentono il rilevamento tempestivo di fonti di pericolo, i dati personali raccolti senza motivo, dall'altro lato, deve esaminare attentamente le informazioni ottenute prima che vengano trasmesse e limitarle nella misura necessaria in conformità con le pertinenti norme di trasmissione.La trasmissione deve essere registrata - a meno che non si tratti di rapporti diretti alla Cancelleria federale o ai singoli ministri federali e del loro uso nella politica del governo - in modo che la conformità ai requisiti di trasmissione possa essere resa accessibile a un controllo indipendente (vedere BVerfGE 141, 220 <340 f. Marg. 322>; vedi anche marginale 291 di seguito. Occorre inoltre menzionare il regolamento giuridico su cui si basa la trasmissione.

230

Ciò non pregiudica la capacità di collegare le informazioni disponibili in vari punti e di avviare il loro scambio utilizzando file composti, come quelli previsti dalla legge antiterrorismo (sui requisiti costituzionali pertinenti BVerfGE 133, 277 <320 ss. Rn. 105 ss.>).

231

7. Requisiti speciali si applicano alla trasmissione di dati a corpi estranei. Inizialmente - indipendentemente da un possibile coinvolgimento nelle cooperazioni - la questione del trasferimento di conoscenze nei singoli casi (per il trasferimento automatizzato di dati nell'ambito delle cooperazioni, vedere i paragrafi 254 e seguenti e 262 e seguenti).

232

a) Da un lato, si applicano i requisiti summenzionati per la protezione degli interessi legali e le soglie di intervento per quanto riguarda la trasmissione di dati alle autorità nazionali (sopra, marginale 216 e seguenti e 220 e seguenti). A tale proposito, al legislatore non è impedito di tenere conto dell'indipendenza dei sistemi giuridici stranieri nella progettazione delle autorizzazioni; tuttavia, ciò non mette in discussione il livello di protezione materiale (cfr. BVerfGE 141, 220 <343 marginale 331>).

233

b) D'altra parte, il trasferimento di dati all'estero, come requisito separato, richiede che venga stabilita una norma di legge relativa al trattamento di corpi estranei con i dati trasmessi ad essi. Ciò tiene conto del fatto che il trattamento dei dati raccolti dalle autorità tedesche dopo la trasmissione all'estero non è più soggetto ai requisiti della Legge fondamentale, poiché le autorità statali straniere sono obbligate a mantenere i propri obblighi legali e, dall'altro, le autorità statali tedesche sono responsabili della trasmissione è vincolato ai diritti fondamentali ed è responsabile della trasmissione (cfr. VerfGE 141, 220 <342 marg. 326 f.>).

234

Secondo la giurisprudenza, i requisiti in materia riguardano, da un lato, la tutela delle garanzie di protezione dei dati (aa) e, dall'altro, la tutela dei diritti umani quando si utilizzano le informazioni (bb) da parte dello stato del destinatario. Entrambi richiedono regole chiare per garantire che il

Servizio di intelligence federale sia adeguatamente assicurato (cc). Inoltre, il mantenimento dei limiti di trasmissione per la trasmissione di dati dal monitoraggio strategico deve essere garantito ottenendo impegni affidabili da parte dei destinatari (dd).

235

aa) Il primo prerequisito mira a salvaguardare le garanzie di protezione dei dati derivanti dal diritto alla privacy. Tuttavia, non è necessario applicare norme comparabili per il trattamento dei dati personali come nell'ordinamento tedesco o che sia garantito lo stesso livello di protezione della Legge fondamentale nel paese destinatario. La Legge fondamentale riconosce piuttosto l'indipendenza e la diversità dei sistemi giuridici e generalmente li rispetta nel contesto dello scambio di dati. Le delimitazioni e le valutazioni non devono corrispondere a quelle del sistema giuridico tedesco e anche della Legge fondamentale tedesca.

236

Tuttavia, la trasmissione dei dati all'estero è consentita solo se il trattamento dei dati trasmessi non pregiudica le garanzie di protezione dei diritti umani dei dati personali. Ciò non significa che le disposizioni istituzionali e procedurali basate sul modello tedesco debbano essere garantite nel sistema giuridico estero; in particolare, le garanzie formali e istituzionali richieste dalla legge tedesca sulla protezione dei dati non devono essere disponibili. In questo senso, è necessario garantire un livello materiale adeguato della legge sulla protezione dei dati per la gestione dei dati trasmessi nel paese destinatario. A questo proposito, è particolarmente importante considerarese per l'uso dei dati i limiti comunicati durante la trasmissione sono almeno fondamentalmente rispettati attraverso obblighi di assegnazione e cancellazione nonché requisiti di base per il controllo e la sicurezza dei dati. Decisivi per questa valutazione sono la legislazione nazionale e gli obblighi internazionali dello Stato beneficiario, nonché la loro attuazione nella pratica di applicazione quotidiana (BVerfGE 141, 220 <344 f. Rn. 334 f.> MwN).).).

237

bb) Inoltre, il trasferimento di dati ad altri paesi è escluso se c'è motivo di temere che l'uso delle informazioni violi i principi fondamentali dello stato di diritto. Lo stato non deve tendere la mano per violare la dignità umana (vedi BVerfGE 140, 317 <347 paragrafo 62>; 141, 220 <342 paragrafo 328>). Per l'uso nel paese destinatario, deve essere garantito che le informazioni non vengano utilizzate lì per persecuzioni politiche, punizioni o trattamenti disumani o degradanti (cfr. L'articolo 16a.3 GG). Il legislatore deve garantire che la protezione della Convenzione europea dei diritti dell'uomo e di altri trattati internazionali sui diritti umani (cfr. Art. 1 cpv.2 GG) trasferendo i dati raccolti dalle autorità tedesche all'estero e ad organizzazioni internazionali (vedere BVerfGE 141, 220 <345 paragrafo 336>). Alla luce delle specificità delle attività di raccolta e trasmissione di informazioni, che possono comprendere anche contatti con Stati che non sono basati sullo stato di diritto, è particolarmente importante garantire che le informazioni non vengano utilizzate per perseguitare determinate fasce della popolazione, per reprimere gli oppositori, per violare i diritti umani o per violare questioni umanitarie Uccidere, torturare o detenere il diritto internazionale senza il giusto processo. Il servizio deve formare e decidere autonomamente quali sono le norme di diritto internazionale pertinenti.Anche a questo proposito, i diritti di informazione devono essere concordati con i paesi beneficiari, il che consente un monitoraggio tracciabile della conformità alle norme internazionali sui diritti umani.

238

cc) Per mantenere questi standard di protezione, è necessario disporre di norme giuridicamente chiare che forniscano al Servizio di intelligence federale una garanzia del livello di protezione all'estero. Prima della trasmissione, il servizio deve garantire il rispetto dei requisiti di protezione dei dati e dei diritti umani.

239

(1) La verifica non richiede un esame individuale completo o impegni individuali vincolanti sotto tutti gli aspetti, ma può inizialmente basarsi su una valutazione fattuale generalizzata della situazione fattuale e giuridica negli Stati beneficiari. Tuttavia, l'esame deve essere progettato in modo tale da rilevare fatti contrastanti e la valutazione può essere scossa (vedere BVerfGE 140, 317 <349 para. 69>). Se non si applicano valutazioni generalizzate, è necessaria una valutazione individuale fattuale, dalla quale consegue che la conformità ai requisiti di base per la gestione dei dati è sufficientemente garantita. Se necessario, possono e devono essere fornite garanzie individuali vincolanti. Una garanzia obbligatoria è generalmente adattaAffrontare eventuali dubbi sull'ammissibilità del trasferimento dei dati, a meno che non si possa prevedere in singoli casi che l'assicurazione non sarà soddisfatta (vedere BVerfGE 63, 215 <224>; 109, 38 <62>; 140, 317 <350 numero marginale 70>). I legislatori possono anche decidere quali requisiti si applicano in dettaglio sulla base di una valutazione caso per caso (BVerfGE 141, 220 <345 f. Marginal 337 f.>).

240

Poiché i dati sono in gran parte raccolti nell'ambito del monitoraggio strategico, indipendentemente dal fatto che la persona interessata sia catturata in una situazione pericolosa da un punto di vista oggettivo, si riferisce anche a circostanze in paesi in cui lo stato di diritto non è protetto e allo stesso tempo è spesso di natura altamente politica Il Servizio di intelligence federale richiede un'attenzione particolare al riguardo. Anche se le valutazioni di determinati paesi possono essere generalmente effettuate in modo generalizzato, è sempre necessario un controllo per l'interessato se vi sono indicazioni che la trasmissione dei dati possa metterli in pericolo in modo specifico. Nella misura in cui la trasmissione riguarda dati di giornalisti, avvocati o altri gruppi professionali meritevoli di protezione,La protezione della riservatezza, che deve essere riconosciuta - anche per evitare di metterli in pericolo - richiede una valutazione indipendente che differisce dalla valutazione basata esclusivamente sull'uso domestico di tali dati (vedere il margine n. 193 ss. Sopra); in linea di principio, deve essere soggetto a revisione giudiziaria preventiva (vedi Ufficio delle Nazioni Unite dell'Alto commissario per i diritti umani, lettera del relatore speciale datata 29 agosto 2016, OL DEU 2/2016, p. 7).Lettera del relatore speciale datata 29 agosto 2016, OL DEU 2/2016, p. 7).Lettera del relatore speciale datata 29 agosto 2016, OL DEU 2/2016, p. 7).

241

(2) Garantire il rispetto del livello di protezione richiesto è una decisione che non è soggetta a libera disposizione politica. Deve basarsi su informazioni sostanziali, realistiche e attuali. Deve essere documentato ed essere accessibile a un'ispezione indipendente (vedere BVerfGE 141, 220 <346 marginale 339>). Per le procedure di trasmissione particolarmente pesanti o difficili da giudicare in relazione ai requisiti legali, possono essere necessarie ulteriori precauzioni procedurali come prenotazioni da parte del capo dell'agenzia o dell'ufficio del cancelliere o - ad esempio per la trasmissione di informazioni su giornalisti o avvocati meritevoli di protezione - un controllo preventivo simile a quello di un tribunale.

242

dd) Poiché i dati raccolti dal Servizio federale di intelligence nel contesto della sorveglianza strategica delle telecomunicazioni si basano su misure di sorveglianza incondizionate, mantenere efficacemente i limiti per la trasmissione di tali conoscenze alle autorità operative, in particolare alle autorità di polizia e di polizia o all'amministrazione nazionale, è di particolare importanza per. Nella misura in cui il Servizio di intelligence federale trasmette le conoscenze ai servizi di intelligence stranieri, si basa - secondo le prassi attuali - a continuare a essere obbligato a rendere tale trasmissione dipendente dalla promessa che il servizio estero trasmetterà le informazioni solo con il consenso del Servizio di intelligence federale. In determinate circostanze, la semplice promessa del servizio estero potrebbe essere sufficienteche queste informazioni personali saranno trasmesse ad altri organismi solo se sono disponibili fatti attendibili, che le persone interessate dalle informazioni sono responsabili di un pericolo specifico e particolarmente grave o sono coinvolte in circostanze oggettive o - nella misura in cui sono trasmesse a servizi di informazione atti di paesi terzi - la spedizione è soggetta a un impegno corrispondente (per impegni nel contesto della cooperazione si vedano i paragrafi 259 e seguenti e 264 seguenti). Come per tutti gli impegni, ciò presuppone che tali impegni possano essere rispettati e che siano affiancati dal diritto all'informazione del Servizio di intelligence federale nei confronti del servizio estero.se esistono fatti attendibili secondo cui le persone interessate dalle informazioni sono responsabili di un pericolo specifico e particolarmente grave o sono coinvolte in circostanze oggettive o - nella misura in cui riguardano l'inoltro a servizi di intelligence di paesi terzi - l'inoltro è soggetto a riserva Viene assunto un impegno appropriato (per impegni nel contesto di collaborazioni, vedere i paragrafi 259 e seguenti e 264 sotto). Come per tutti gli impegni, ciò presuppone che tali impegni possano essere rispettati e che siano affiancati dal diritto all'informazione del Servizio di intelligence federale nei confronti del servizio estero.se esistono fatti attendibili secondo cui le persone interessate dalle informazioni sono responsabili di un pericolo specifico e particolarmente grave o sono coinvolte in circostanze oggettive o - nella misura in cui riguardano l'inoltro a servizi di intelligence di paesi terzi - l'inoltro è soggetto a riserva Viene assunto un impegno appropriato (per impegni nel contesto di collaborazioni, vedere i paragrafi 259 e seguenti e 264 sotto). Come per tutti gli impegni, ciò presuppone che tali impegni possano essere rispettati e che siano affiancati dal diritto all'informazione del Servizio di intelligence federale nei confronti del servizio estero.che le persone interessate dalle informazioni sono responsabili di un pericolo specifico e particolarmente grave o sono coinvolte in circostanze oggettive o - nella misura in cui sono inoltrate a servizi di intelligence di paesi terzi - l'inoltro è subordinato a una corrispondente promessa (Impegni nel contesto di collaborazioni, vedi marg. 259 e seguenti e 264 sotto. Come per tutti gli impegni, ciò presuppone che tali impegni possano essere rispettati e che siano affiancati dal diritto all'informazione del Servizio di intelligence federale nei confronti del servizio estero.che le persone interessate dalle informazioni sono responsabili di un pericolo specifico e particolarmente grave o sono coinvolte in circostanze oggettive o - nella misura in cui sono inoltrate a servizi di intelligence di paesi terzi - l'inoltro è subordinato a una corrispondente promessa (Impegni nel contesto di collaborazioni, vedi marg. 259 e seguenti e 264 sotto. Come per tutti gli impegni, ciò presuppone che tali impegni possano essere rispettati e che siano affiancati dal diritto all'informazione del Servizio di intelligence federale nei confronti del servizio estero.

IV.

243

La progettazione di regolamenti che aprono la sorveglianza strategica delle telecomunicazioni per la cooperazione con i servizi di intelligence stranieri presenta particolari sfide costituzionali. Nel contesto di tali cooperazioni, il legislatore desidera consentire al Servizio di intelligence federale di valutare il traffico di dati che ha registrato utilizzando termini di ricerca determinati da altri servizi di intelligence e di inoltrare automaticamente i relativi risultati. Inoltre, i dati sul traffico dovrebbero

essere trasmessi ai partner della cooperazione senza un'analisi preliminare. Viceversa, anche il Servizio di intelligence federale dovrebbe essere autorizzato a utilizzare i dati e le capacità di altri servizi.Nel complesso, la base di dati per l'uso dei termini di ricerca dovrebbe essere ampliata e le capacità utilizzate in modo più efficace in uno scambio reciproco (cfr. BTDrucks 18/9041, p. 29).

244

Tali regolamenti possono soddisfare i requisiti legali di base solo se i limiti legali della sorveglianza strategica non sono sovrastati dallo scambio reciproco e la responsabilità del Servizio di intelligence federale per i dati che raccoglie e valuta è sostanzialmente preservata (cfr. Gusy, in: Schenke / Graulich / Ruthig [ed.], Legge federale sulla sicurezza, 2a edizione 2019, § 1 BNDG Rn. 64).

245

1. In quanto ordine internazionale rispettoso della legge, la Legge fondamentale è aperta a tale cooperazione tra i servizi di intelligence. Tuttavia, richiede norme proprie che garantiscano la tutela dei diritti fondamentali anche nel contesto della cooperazione internazionale tra i servizi di intelligence.

246

a) Con il preambolo, Art. 1 Paragrafo 2, Art. 9 Paragrafo 2, Art. 16 Paragrafo 2, Art. 23-26 e Art. 59 Paragrafo 2 GG, la Legge fondamentale lega la Repubblica Federale in modo completo alla comunità internazionale e ha programmaticamente orientato l'autorità pubblica tedesca verso la cooperazione internazionale (vedi BVerfGE 141, 220 <341 f. margine n. 325> mwN). Questo vale anche per garantire la sicurezza. La Corte costituzionale federale ha sottolineato che la più efficace cooperazione possibile con le autorità di sicurezza di altri paesi può essere particolarmente importante per questo.Uno scambio di informazioni funzionante può, nell'interesse della protezione costituzionalmente richiesta delle persone, richiedere il trasferimento delle conoscenze ottenute in Germania e, in cambio, dipendere da informazioni provenienti da corpi estranei (cfr. Verf 141, 220 <268 par. 102>).

247

Di conseguenza, la legge di base è aperta alla cooperazione tra il servizio di intelligence federale e altri servizi di intelligence. Tale cooperazione internazionale può essere di grande importanza per la tutela degli interessi della politica estera e di sicurezza della Repubblica federale e, in questo contesto, per la prevenzione dei pericoli e può essere collegata all'apertura internazionale della Legge fondamentale (vedi anche BVerfGE 143, 101 <152 ff. marginale 168 ff.>). Di conseguenza, il Servizio federale di intelligence può anche essere autorizzato a utilizzare i propri poteri per gli interessi di informazione di servizi e stati stranieri. È essenziale che questi siano comparabili a un legittimo interesse educativo del Servizio federale di intelligence e che siano compatibili con gli interessi di politica estera e di sicurezza della Repubblica federale.Inoltre, l'uso dei dati deve essere integrato in un quadro giuridico.

248

b) La cooperazione nel campo della sorveglianza delle telecomunicazioni deve tuttavia essere concepita in modo tale da non compromettere la protezione dei diritti fondamentali contro le misure di sorveglianza segreta e i relativi requisiti per la raccolta, l'elaborazione e la trasmissione dei dati. Ciò vale in particolare per la protezione contro la sorveglianza domestica, che non deve essere

privata della sua efficacia attraverso un libero scambio di informazioni dalle misure di sorveglianza relative ai servizi stranieri collegati alla Germania. Tale "scambio di suoneria" non è consentito dalla legge costituzionale. Lo stesso vale, tuttavia, per i requisiti legali di base del Servizio di intelligence federale in materia di servizi di telecomunicazione all'estero.

249

In base a ciò, ai servizi esteri stessi può essere concesso nella migliore delle ipotesi il diritto di attuare misure di sorveglianza all'interno del paese, oppure può essere data una promessa di tolleranza se esiste un motivo specifico per questo e la validità illimitata della protezione dei diritti fondamentali è garantita in termini di legge materiale, procedura e procedura attraverso basi legali dettagliate. Dalla dimensione protettiva dei diritti fondamentali ne consegue che lo stato tedesco deve proteggere le persone soggette alla protezione del proprio sistema giuridico in Germania dalle misure di sorveglianza di altri Stati che violano i diritti fondamentali (cfr. Gusy, in: Schenke / Graulich / Ruthig [ed.], Legge federale sulla sicurezza, 2a edizione 2019, § 1 margine BNDG n. 62). Le cooperazioni non possono essere esentate da questo.

250

c) Per il resto, la cooperazione con i servizi di intelligence esteri richiede una propria base giuridica. I regolamenti sono necessari, da un lato, per consentire al Federal Intelligence Service di accedere alle opzioni di monitoraggio di altri servizi e all'acquisizione e all'utilizzo dei dati da essi raccolti. A questo proposito, la trasmissione dei termini di ricerca da parte del Servizio di intelligence federale a un servizio estero per l'uso e la valutazione, nonché il recupero o l'accettazione da parte dei partner di database o flussi di dati messi a disposizione dei partner per la propria valutazione da parte del Servizio di intelligence federale tramite selettori o altre tecniche di analisi (cfr. Requisiti di tali regolamenti anche EGMR, Big Brother Watch e altri c. Regno Unito, sentenza del 13 settembre 2018, n. 58170/13 e altri,Sezione 424). Nel fare ciò, si deve tener conto del potenziale intrinseco di tali pratiche di elusione dei legami nazionali (cfr. Anche CEDU, loc. Cit.) E delle minacce specifiche ai diritti fondamentali che possono derivare dalla cooperazione. È particolarmente importante regolare la misura in cui il Servizio di intelligence federale può ricevere e utilizzare le informazioni personali da servizi stranieri nell'ambito di cooperazioni, per le quali vi sono indicazioni che sono state ottenute monitorando le comunicazioni interne tedesche. Poiché il legislatore non ha ancora creato tali regolamenti, i requisiti pertinenti non sono oggetto di questa procedura.) e le minacce specifiche ai diritti fondamentali che possono derivare dalla cooperazione. È particolarmente importante regolare la misura in cui il Servizio di intelligence federale può ricevere e utilizzare le informazioni personali da servizi stranieri nell'ambito di cooperazioni, per le quali vi sono indicazioni che sono state ottenute monitorando le comunicazioni interne tedesche. Poiché il legislatore non ha ancora creato tali regolamenti, i requisiti pertinenti non sono oggetto di questa procedura.) e le minacce specifiche ai diritti fondamentali che possono derivare dalla cooperazione. È particolarmente importante regolare la misura in cui il Servizio di intelligence federale può ricevere e utilizzare le informazioni personali da servizi stranieri nell'ambito di cooperazioni, per le quali vi sono indicazioni che sono state ottenute monitorando le comunicazioni interne tedesche. Poiché il legislatore non ha ancora creato tali regolamenti, i requisiti pertinenti non sono oggetto di questa procedura.la misura in cui il Servizio di intelligence federale può ricevere e utilizzare le informazioni personali da servizi stranieri nell'ambito di cooperazioni, per le quali vi sono indicazioni che sono state ottenute monitorando le comunicazioni interne tedesche. Poiché il legislatore non ha ancora creato tali regolamenti, i requisiti pertinenti non sono oggetto di questa procedura.la misura in cui il Servizio di intelligence federale può ricevere e utilizzare le informazioni personali da servizi stranieri nell'ambito di cooperazioni, per le quali vi sono indicazioni che sono state ottenute monitorando le comunicazioni interne tedesche. Poiché il

legislatore non ha ancora creato tali regolamenti, i requisiti pertinenti non sono oggetto di questa procedura.

251

D'altro canto, le norme sono richieste nella misura in cui al Servizio di intelligence federale devono essere attribuiti poteri di sorveglianza e trasmissione, che può anche essere utilizzato nell'interesse e sotto la guida di altri servizi. Se il legislatore desidera consentire al Servizio di intelligence federale di valutare i dati raccolti utilizzando i termini di ricerca dei partner della cooperazione o la trasmissione automatizzata di dati di contenuto preselezionati o dati di traffico non selezionati a servizi stranieri, deve creare una propria base giuridica per questo, come fa con § 14, 15 BNDG in linea di principio.

252

2. I requisiti costituzionali da porre su tali basi giuridiche mirano a garantire che i limiti dei diritti fondamentali generalmente sviluppati per il monitoraggio strategico siano preservati nel modo più efficace possibile anche nel contesto della cooperazione.

253

Poiché tale cooperazione può essere considerata solo sotto la stretta protezione della comunicazione interna, deve essere limitata ai dati dell'intelligence estera-straniera (sopra, marginale 170 e seguenti). Al fine di salvaguardare la protezione dei diritti fondamentali garantiti dall'articolo 10, paragrafo 1, della legge di base, è necessario innanzitutto garantire, nell'ambito delle cooperazioni per la raccolta e l'elaborazione dei dati da parte del servizio di intelligence federale, che i dati di telecomunicazione di residenti e cittadini tedeschi vengano filtrati ove possibile e altrimenti immediatamente separati in caso di successiva identificazione . Ciò include un corrispondente filtraggio dei termini di ricerca adottati dai servizi dei partner, nonché il filtraggio dei dati forniti per la trasmissione automatizzata a partner stranieri (vedere sotto i paragrafi 255 e seguenti e 264).I requisiti sviluppati per questo (margine 170 e seguenti) si applicano anche qui. Inoltre, il legislatore deve anche specificare gli scopi per i quali è consentita la sorveglianza nell'interazione dei servizi per la cooperazione, con sufficiente precisione e standard, e limitarlo alla protezione di beni comuni di alto livello (margine n. 175 f. Sopra). Analogamente, le collaborazioni devono essere suddivise sulla base di una definizione formalizzata di misure di sorveglianza differenziate in base all'obiettivo, al soggetto e alla durata e da strutturare secondo il diritto procedurale (punti 178 e seguenti). Ciò non esclude l'inclusione di tali misure di sorveglianza attuate congiuntamente, ciascuna definita, in una cooperazione a più lungo termine e più ampia, se necessario sulla base di possibili accordi quadro.Come la trasmissione di conoscenze individuali, anche la trasmissione automatizzata di dati richiede una garanzia documentata che i dati trasmessi siano gestiti in conformità con lo stato di diritto (margine n. 233 ss. Sopra). La verifica deve essere garantita una volta per ciascuna delle misure di controllo attuate congiuntamente; se vi è motivo di farlo nel corso della cooperazione, è necessario aggiornarlo (sulla necessità di impegni che hanno un loro significato nel contesto della cooperazione, cfr. marg. 259 ss. e 264 in appresso).se vi è motivo di farlo nel corso della cooperazione, è necessario aggiornarlo (sulla necessità di impegni che hanno un loro significato nel contesto della cooperazione, cfr. marg. 259 ss. e 264 in appresso).se vi è motivo di farlo nel corso della cooperazione, è necessario aggiornarlo (sulla necessità di impegni che hanno un loro significato nel contesto della cooperazione, cfr. marg. 259 ss. e 264 in appresso).

254

3. Requisiti specifici si applicano nella misura in cui il Servizio di intelligence federale intende utilizzare i termini di ricerca nell'ambito di cooperazioni che sono state determinate da un servizio di intelligence straniero e gli hit vengono quindi trasmessi automaticamente al servizio partner senza ulteriore analisi del contenuto. A questo proposito, il legislatore deve creare norme che garantiscano la responsabilità legale fondamentale del Servizio di intelligence federale per i dati raccolti e il loro trattamento.

255

a) Per questo, è prima necessario controllare attentamente i termini di ricerca utilizzati per il servizio partner e i relativi casi di successo. Il Servizio federale di intelligence deve verificare sia i termini di ricerca stessi sia i dati che filtrano per determinare se il loro utilizzo è soggetto a diritti fondamentali.

256

aa) Per quanto riguarda i termini di ricerca determinati dai servizi partner, è prima necessario - in base alla pratica precedente - verificare se questi sono finalizzati ai fini della misura di monitoraggio specificata in ciascun caso. Ciò richiede un controllo di plausibilità sufficiente dei termini di ricerca da parte dei servizi partner. Inoltre, sia per quanto riguarda i termini di ricerca sia per quanto riguarda gli hit, deve essere fornito un controllo - ad esempio basato su elenchi di persone a rischio - che sia finalizzato a dati provenienti da persone o da situazioni in cui vi sono indicazioni di un particolare bisogno di protezione, come ad esempio Se possibile, i dissidenti persistenti oi cosiddetti informatori possono essere filtrati.Come già accade per quanto riguarda gli interessi o gli obiettivi nazionali nell'Unione europea, sono anche necessarie misure di protezione speciali in materia di diritti fondamentali.

257

Lo stesso vale per le persone le cui attività richiedono un livello speciale di riservatezza, in particolare per avvocati e giornalisti che meritano protezione. Tuttavia, le misure di monitoraggio non sono escluse nel loro insieme nel quadro delle cooperazioni. Tuttavia, anche qui, possono essere ammessi solo in relazione alla protezione legale qualificata della proprietà e in conformità con le soglie di intervento e un compromesso (vedere il margine n. 194 ss. Sopra). Al fine di controllare questi requisiti, i termini di ricerca che mirano a catturare le telecomunicazioni di tali persone devono prima essere identificati, se possibile, come parte dei processi di filtraggio, prima di essere sottoposti a un controllo manuale, inclusa la necessaria considerazione. Per la domandaSe i requisiti per l'uso di tali selettori sono soddisfatti, il controllo di plausibilità deve essere eseguito dal servizio partner. Di conseguenza, il traffico di dati registrato dai termini di ricerca deve essere verificato prima di essere trasmesso automaticamente al servizio estero per determinare se - in base alle conoscenze disponibili al Servizio di intelligence federale - possono essere assegnati a persone la cui comunicazione richiede anche una riservatezza speciale per evitare la repressione statale e, se necessario, manualmente dai un'occhiata. Se le decisioni individuali devono essere prese al riguardo, devono essere sottoposte a controllo giurisdizionale preventivo.Di conseguenza, il traffico di dati registrato dai termini di ricerca deve essere verificato prima di essere trasmesso automaticamente al servizio estero per determinare se - in base alle conoscenze disponibili al Servizio di intelligence federale - possono essere assegnati a persone la cui comunicazione richiede anche una riservatezza speciale per evitare la repressione statale e, se necessario, manualmente dai un'occhiata. Se le decisioni individuali devono essere prese al riguardo, devono essere sottoposte a controllo giurisdizionale preventivo.Di conseguenza, il traffico di dati registrato dai termini di ricerca deve essere verificato prima di essere trasmesso automaticamente al servizio estero per

determinare se - in base alle conoscenze disponibili al Servizio di intelligence federale - possono essere assegnati a persone la cui comunicazione richiede anche una riservatezza speciale per evitare la repressione statale e, se necessario, manualmente dai un'occhiata. Se le decisioni individuali devono essere prese al riguardo, devono essere sottoposte a controllo giurisdizionale preventivo.e controllare manualmente se necessario. Se le decisioni individuali devono essere prese al riguardo, devono essere sottoposte a controllo giurisdizionale preventivo.e controllare manualmente se necessario. Se le decisioni individuali devono essere prese al riguardo, devono essere sottoposte a controllo giurisdizionale preventivo.

258

bb) Questo controllo deve essere effettuato nel modo più efficace possibile. In connessione con la pratica precedente, un controllo automatizzato può essere considerato per primo. Il Servizio di intelligence federale è legalmente obbligato a utilizzare i risultati e l'esperienza del proprio lavoro per raccogliere qualsiasi indicazione di particolare vulnerabilità e vulnerabilità di determinate persone e per combinare gli identificativi di telecomunicazione correlati in un modo che consenta di filtrare i termini di ricerca e i dati forniti per la trasmissione. Lo stesso vale per gli identificatori di giornalisti, avvocati o simili persone, gruppi o istituzioni la cui comunicazione è particolarmente riservata. I database e i processi di filtro pertinenti devono essere costantemente aggiornati e ulteriormente sviluppati.Se necessario, i processi automatizzati basati su campioni sufficientemente grandi devono essere integrati da un controllo manuale. In ogni caso, sulla base delle attuali prestazioni del processo automatizzato, sulla base dei risultati dell'audizione, ciò dovrebbe attualmente essere indispensabile.

259

b) Garantire impegni sostanziali è di particolare importanza per la trasmissione automatizzata di dati valutati in modo incompleto a servizi esteri. Poiché la valutazione dei dati raccolti dal servizio tedesco è affidata a un servizio straniero, che a sua volta non è vincolato dalla Legge fondamentale, è necessario ottenere impegni specifici dai servizi partner per l'ulteriore trattamento dei dati. In considerazione della validità dei diritti fondamentali, gli impegni devono ora essere assunti anche all'estero per proteggere i diritti fondamentali delle persone monitorate.

260

In base a ciò, è necessario prima richiedere ai servizi partner di eliminare il traffico di dati che coinvolge cittadini o cittadini tedeschi il più presto possibile, a condizione che siano identificati come tali nella valutazione. D'altro canto, sono necessari impegni sostanziali per gestire le relazioni riservate che richiedono protezione. Infine, gli impegni devono anche essere ottenuti qui per garantire che i limiti di trasmissione applicabili al Servizio di intelligence federale non siano compromessi dai servizi partner (paragrafo 242 sopra).

261

In conformità con lo stato di diritto generale, tali impegni devono essere collegati alle misure di sorveglianza definite individualmente e rinnovati se necessario. Non devono essere realizzati in una forma giuridicamente vincolante, ma devono effettivamente essere efficaci. Il governo federale deve verificare fino a che punto tali accordi possono essere affiancati da diritti di informazione o obblighi di notifica nonché da regolamenti di comunicazione e azione - come una richiesta di cancellazione - che il servizio potrebbe e potrebbe dover utilizzare.

262

4. Infine, è necessario un regolamento separato nella misura in cui tutti i dati sul traffico devono essere trasmessi a servizi di intelligence stranieri nell'ambito di cooperazioni senza selezione preventiva basata su determinati termini di ricerca, in modo che questi possano essere archiviati e valutati con i loro mezzi.

263

a) Dato che il Servizio di intelligence federale consegna i dati raccolti senza ulteriori controlli, è necessario disporre di restrizioni specifiche per tale forma di cooperazione. Una trasmissione globale di dati sul traffico non può essere consentita in modo continuo e solo come guida finale, ma richiede una qualificata necessità di chiarimenti in merito a una situazione di rischio specificatamente specificata. A tale proposito, oltre all'esistenza di situazioni di rischio generale dovute a determinati eventi, devono esserci motivi per contrastare minacce specifiche mediante misure educative e per garantire la capacità della Repubblica federale di agire. Questo può essere il caso, ad esempio, se ci sono indicazioni reali per la preparazione di attacchi terroristici,per lo spostamento di armi da guerra su una determinata rotta o per attacchi informatici coordinati contro determinati stati o istituzioni. Nel contesto della definizione formalizzata della misura (margine n. 179 e seguenti), ciò dovrebbe essere notato e la valutazione da parte del servizio estero limitata a questo obiettivo. La definizione di tale misura deve essere accessibile a un controllo giurisdizionale.

264

b) Inoltre, in conformità con le disposizioni generali (margine n. 170 ss. sopra), i dati dei cittadini e dei residenti tedeschi devono essere prima filtrati dai dati sul traffico. I dati di telecomunicazione delle persone che sono note al Servizio di intelligence federale come particolarmente meritevoli di protezione e bisognosi di protezione devono essere separati qui (margine n. 257 f. Sopra). I requisiti per la garanzia dello stato di diritto rimangono comunque inalterati (vedi nm. 233 ss. Sopra). Gli impegni da ottenere dai servizi esteri includono anche il fatto che i dati trasmessi nel loro insieme non siano conservati per più di sei mesi. Inoltre, il governo federale deve esaminarese i limiti legali fondamentali della sorveglianza e dell'uso dei dati possano essere ulteriormente garantiti per la forma di cooperazione richiedendo impegni aggiuntivi.

v.

265

Il principio di proporzionalità impone inoltre requisiti in materia di trasparenza, protezione giuridica individuale e controllo delle misure di sorveglianza (cfr. VerfGE 141, 220 <282 ss. Marginale 134 ss.> MwN; stRspr). In termini di trasparenza e protezione giuridica individuale, tuttavia, questi sono stati notevolmente ridotti ai fini dell'educazione alle telecomunicazioni estere. Per compensare ciò, il principio di proporzionalità mostra requisiti speciali per un controllo indipendente ai sensi della legge oggettiva (vedere BVerfGE 133, 277 <369 marginale 214>; 141, 220 <284 f. Margine 140 f.>).

266

1. I requisiti per garantire la trasparenza del trattamento dei dati comprendono le richieste di informazioni. In linea di principio, ciò vale anche per i servizi di informazione (vedi BVerfGE 125, 260 <331 f.>). Tuttavia, queste affermazioni possono essere limitate nella misura in cui sono

indispensabili per una efficace esecuzione dei compiti (cfr. BVerfGE 133, 277 <367 f. Margine 209 ss.>; 141, 220 <283 margine n. 137>). Poiché le informazioni all'estero si basano in gran parte sulla riservatezza, il diritto all'informazione degli interessati può quindi essere limitato in misura considerevole. In particolare, è possibile escludere informazioni su come sono stati ottenuti i dati in dettaglio. Se il diritto all'informazione consente la trasparenza solo in misura limitata e può fornire una base per la protezione giuridica individuale,Ciò deve essere compensato da un sistema di controllo dell'obiettivo indipendente ampliato (vedere BVerfGE 133, 277 <369 margine n. 214>; ulteriori dettagli sul margine n. 272 e seguenti).

267

2. I requisiti per la progettazione proporzionata di misure di sorveglianza segreta - da parte dei servizi di intelligence e da parte di altre autorità di sicurezza - continuano a includere obblighi di notifica. Anche in questo caso il legislatore può prevedere eccezioni in considerazione delle attività legali costituzionalmente protette di terzi e garantire che i compiti vengano svolti in modo efficace. Sebbene queste eccezioni debbano essere limitate a ciò che è assolutamente necessario (vedere BVerfGE 109, 279 <364>; 125, 260 <336>; 141, 220 <283 paragrafo 136>), i requisiti di notifica relativi al monitoraggio strategico non vanno molto oltre.

268

a) Per quanto riguarda le persone in Germania, tuttavia, è necessario anche un monitoraggio strategico delle normative differenziate che assicurino la notifica il più possibile. Ciò è particolarmente importante se, nonostante i meccanismi di filtro esistenti, la comunicazione con la partecipazione di residenti o tedeschi non è tecnicamente separata, ma è riconosciuta solo come parte della valutazione manuale e non viene immediatamente cancellata.

269

Al contrario, il legislatore può in genere astenersi dagli obblighi di notifica per le misure di monitoraggio strategico all'estero (vedi Marxsen, DÖV 2018, p. 218 <227>; Dietrich, in: Schenke / Graulich / Ruthig [ed.], Sicherheitsrecht des Federale, 2a edizione 2019, § 6 BNDG Rn.10). Per le attività del Servizio di intelligence federale che hanno un impatto diretto o si svolgono all'estero, vi è un interesse elementare nel garantire che queste rimangano inosservate nel complesso in modo che il servizio possa svolgere i suoi compiti in modo permanente. Qualsiasi divulgazione formalmente motivata della presenza o opzioni di chiarimento del servizio in un altro stato può mettere in pericolo le sue fonti in particolare (vedi Gusy, in: Schenke / Graulich / Ruthig [ed.], Federal Security Law, 2nd edition 2019, BNDG Prep. Marg.10). Al contrario, la notifica di persone che vivono all'estero può svolgere la propria funzione solo in misura molto limitata. Né la fornitura di protezione legale praticamente realizzabile (vedi BVerfGE 65, 1 <70>; 109, 279 <363 f.; 367>; 120, 351 <361>; stRspr), né l'obiettivo di creare fiducia nel pubblico, ancora la funzione di consentire un discorso democratico su tali misure (cfr. VerfGE 125, 260 <335 f.>; 133, 277 <366 paragrafo 206>; 141, 220 <282 f. paragrafo 135 f.>; stRspr) , può essere ottenuto tramite notifiche all'estero in modo analogo a quello in Germania. Piuttosto, una notifica può persino essere pericolosa per le persone colpite nell'altro sistema legale,perché li espone all'attenzione e alla sfiducia delle proprie autorità o, se necessario, di terzi.

270

Di conseguenza, i requisiti relativi alla trasparenza dell'azione del governo e alla possibilità pratica di ottenere la protezione giuridica individuale sono stati notevolmente ridotti. Sebbene l'apertura del

ricorso legale ai sensi delle sezioni 40, 50, paragrafo 1, n. 4, VwGO rimanga formalmente inalterata, a causa della mancanza di conoscenza delle misure di sorveglianza, la protezione giuridica per le persone colpite può essere ottenuta solo in rari casi eccezionali. Anche a questo proposito, al fine di mantenere la proporzionalità della compensazione, è necessario un controllo giuridico oggettivo ampliato e indipendente (sotto il margine n. 272 ss.).

271

b) Se la legge non prevede requisiti di notifica, si può osservare l'articolo 10.2 frase 2 della Legge fondamentale. Tuttavia, ciò non porta a restringere i requisiti costituzionali per la creazione del disegno di legge organizzativa di un controllo giuridico oggettivo. Il suo campo di applicazione è già strettamente limitato in termini di caratteristiche "protezione del libero ordine democratico di base" e "esistenza o sicurezza del governo federale o di uno stato" (vedi BVerfGE 100, 313 <397 f.>). Anche nella misura in cui sono soddisfatti i requisiti di cui all'articolo 10.2 frase 2 della Legge fondamentale, non vi è alcuna guida organizzativa dettagliata dal suo riferimento agli organi o organi ausiliari nominati dall'organismo rappresentativo del popolo. L'unico requisito èche l'organo di controllo incaricato della revisione debba essere creato dal parlamento e che i suoi membri debbano essere determinati dal parlamento, tenendo così conto delle varie direzioni politiche rappresentate in parlamento. Tuttavia, l'organismo di vigilanza può essere formato all'interno o all'esterno del parlamento (vedi BVerfGE 30, 1 <23>; 143, 1 <12 para 39>). Di conseguenza, non è necessariamente associato ai membri del Bundestag. Né un'indipendenza organizzativa con rigide regole di riservatezza è esclusa dal parlamento (per quanto riguarda la responsabilità parlamentare del Servizio di intelligence federale che segue i suoi principi, che non è oggetto del presente procedimento, vedi BVerfGE 143, 101 <133 ss. Marginale n. 106 ss.>)).Il corpo può anche essere progettato come istituzione indipendente all'interno dell'area funzionale dell'esecutivo (cfr. VerfGE 30, 1 <28>; 143, 1 <12 para 39>; maggiori dettagli sui requisiti di progettazione e possibilità di seguito, paragrafo 274 ss.).

272

3. In base a ciò, la sorveglianza strategica delle telecomunicazioni è compatibile con i requisiti di proporzionalità solo se affiancata da un controllo giuridico oggettivo ampliato e indipendente. Ciò si applica al monitoraggio strategico e all'utilizzo associato dei dati stessi, nonché alla trasmissione delle conoscenze acquisite con esso e alla relativa cooperazione con i servizi esteri. Il controllo deve essere progettato come un controllo legale continuo che consente un accesso completo al controllo. Ha lo scopo di salvaguardare i diritti fondamentali delle persone colpite ed è finalizzato a garantire e rendere praticamente pratici i limiti legali delle attività di sorveglianza del governo.

273

a) I requisiti costituzionali per la progettazione del controllo obiettivo sono particolarmente elevati e dettagliati per quanto riguarda il monitoraggio strategico. Perché il controllo può compensare il fatto che le solite salvaguardie previste dallo Stato di diritto falliscono in larga misura. A questo proposito, ha due funzioni da svolgere: in primo luogo, deve compensare il deficit di protezione legale a causa della debolezza effettiva delle opzioni di protezione giuridica individuali. Poiché il chiarimento delle telecomunicazioni estere richiede solo informazioni e notifiche molto limitate a causa della sua necessità di riservatezza e pertanto difficilmente si può ottenere una protezione giuridica individuale, ciò deve essere compensato da un organismo indipendente con controllo giuridico oggettivo.D'altra parte, come compensazione per l'orientamento essenzialmente unico finale dei poteri di vigilanza, deve garantire la strutturazione procedurale del trattamento di tali

poteri. Contrasta quindi la vasta gamma di opzioni disponibili per il servizio di intelligence federale e garantisce che queste siano razionalizzate proceduralmente in linea con gli obiettivi statutari.

274

b) Devono essere garantiti due diversi tipi di controllo, che devono riflettersi anche nel diritto organizzativo.

275

aa) Da un lato, deve essere garantito un controllo da parte di un organo giudiziario. A tale scopo devono essere previsti organi di arbitrato, che sono dotati di persone che sono, per così dire, indipendenza giudiziaria e che decidono in procedure formalizzate per iscritto e infine con effetto per il governo federale e il servizio di intelligence. Questo controllo deve adempiere al compito protettivo che altrimenti appartiene alla riserva del giudice e alle successive opzioni di protezione legale, in particolare le azioni dichiarative. Di conseguenza, deve consentire un esame basato sul singolo caso, che è equivalente in termini di materiale e procedura a un controllo giudiziario, in particolare almeno altrettanto efficace (cfr. BVerfGE 30, 1 <23>, lì per l'articolo 10.2 frase 2 GG) .

276

bb) D'altra parte, deve essere istituito un controllo giuridico indipendente di natura amministrativa. A questo proposito, deve essere creata un'autorità di controllo in grado di testare in modo indipendente il processo strategico giuridico nel suo complesso - sia le decisioni individuali e le sequenze procedurali, sia la progettazione dei processi di elaborazione e filtro dei dati, nonché gli aiuti tecnici utilizzati per questo. Questa autorità di controllo non deve disporre dell'autorità decisionale finale, ma è sufficiente un diritto di opposizione. Tuttavia, al fine di chiarire le questioni giuridiche di base, deve essere in grado di chiamare l'organo decisionale giudiziario (sulla necessità di poter contattare il Parlamento e il pubblico a determinate condizioni, paragrafo 298 di seguito).

277

c) Il legislatore è responsabile della progettazione dettagliata dell'interblocco delle competenze di controllo in vista dei diversi tipi di controllo. Ha un notevole margine di manovra qui, ma è soggetto alle disposizioni del principio di proporzionalità.

278

aa) Deve garantire che le fasi procedurali essenziali del monitoraggio strategico e del relativo trattamento dei dati siano soggette a un controllo giudiziario con poteri decisionali finali. In particolare, come si evince dai requisiti materiali di cui sopra, la formalizzazione delle varie misure di monitoraggio, anche in materia di cooperazione, le disposizioni specifiche della rete, l'uso dei termini di ricerca, nella misura in cui sono rivolti specificamente alle persone che sono una possibile fonte di pericolo nelle immediate vicinanze Il servizio di notizie è interessato all'utilizzo di termini di ricerca rivolti specificamente alle persone la cui comunicazione gode di una speciale protezione della riservatezza,le decisioni di ponderazione necessarie per proteggere tali rapporti di riservatezza, il trattamento dei dati che possono essere soggetti all'area centrale della vita privata, i trasferimenti che richiedono un controllo speciale, in particolare a uffici esteri, nonché i prerequisiti per stabilire una cooperazione per la trasmissione automatizzata dei dati sul traffico per l'archiviazione e la valutazione servizi esteri. Un controllo a livello di tribunale richiede anche l'uso eccezionale dei dati con riferimento a situazioni pericolose speciali, sebbene siano dati provenienti

dalle telecomunicazioni con la partecipazione di tedeschi o residenti - riconosciuti solo nella valutazione manuale - oppure i dati provengono da misure di sorveglianza che non sono a fini sulla base di un allarme tempestivo,ma furono organizzati in modo indipendente esclusivamente per l'informazione politica del governo federale. Per quanto riguarda la misura in cui tale controllo ha luogo ex ante o ex post e in quest'ultimo caso - se necessario in collaborazione con l'autorità di controllo amministrativa - solo su base casuale, il legislatore ha un campo di applicazione. Certamente anche questo - come si può vedere in parte dalle altre disposizioni sviluppate sopra - è vincolato dal principio di proporzionalità, che in ogni caso richiede un controllo preventivo in merito alle decisioni fondamentali.In quale misura tale controllo ex ante o ex post e in quest'ultimo caso - se necessario in collaborazione con l'autorità di controllo amministrativa - avvenga solo su base casuale, il legislatore ha un campo di applicazione. Certamente anche questo - come si può vedere in parte dalle altre disposizioni sviluppate sopra - è vincolato dal principio di proporzionalità, che in ogni caso richiede un controllo preventivo in merito alle decisioni fondamentali.In quale misura tale controllo ex ante o ex post e in quest'ultimo caso - se necessario in collaborazione con l'autorità di controllo amministrativa - avvenga solo su base casuale, il legislatore ha un campo di applicazione. Certamente anche questo - come si può vedere in parte dalle altre disposizioni sviluppate sopra - è vincolato dal principio di proporzionalità, che in ogni caso richiede un controllo preventivo in merito alle decisioni fondamentali.

279

bb) Nell'interazione delle autorità di controllo, è necessario garantire che l'intero processo di monitoraggio strategico, compresi l'elaborazione e la trasmissione dei dati ad esso collegate, nonché la cooperazione con i servizi di intelligence esteri, siano potenzialmente soggetti a un controllo globale. Se non viene fornito alcun controllo giurisdizionale, deve essere aperta la possibilità di controllo amministrativo. A questo proposito, ovviamente, è necessario solo verificare la legittimità oggettiva delle misure. Ciò non influisce sulla decisione relativa all'adeguato esercizio professionale dei poteri nell'ambito delle disposizioni di legge.

280

cc) Per quanto riguarda il controllo giudiziario, il legislatore dovrà anche verificare se alle persone che possono essere state plausibilmente colpite da misure di sorveglianza possa essere concesso il diritto di avviare un controllo giuridico oggettivo al riguardo con i propri diritti procedurali. Nell'ambito del controllo giuridico oggettivo in questione, che non deve essere inteso come una realizzazione della garanzia costituzionale di protezione giuridica e che non pregiudica l'apertura formale del ricorso legale ai sensi delle sezioni 40, 50, paragrafo 1 n. 4 VwGO, la costituzione è soggetta a un accordo come una procedura esclusione almeno parziale dell'interessato e del pubblico (a porte chiuse) non in anticipo. In ogni caso, questo vale se è necessaria l'esclusioneal fine di aprire un controllo in questo modo che altrimenti non sarebbe possibile e non sarebbe quindi costituzionalmente richiesto (cfr. su tali procedure di reclamo secondo la situazione legale nel Regno Unito Leigh, in: Dietrich / Sule [ed.], Legge sull'Intelligence e Politiche in Europa, 2019, p. 553 <575 ss.>; Vedere anche i commenti sullo stato della vittima dei denuncianti e sulla disponibilità di rimedi interni in EGMR, Big Brother Watch e altri c. Regno Unito, sentenza del 13 settembre 2018, n. 58170 / 13 e altri, §§ 249 e seguenti).575 e seguenti>; vedere anche i commenti sullo stato della vittima dei denuncianti e sulla disponibilità di rimedi interni in EGMR, Big Brother Watch e altri v. Regno Unito, sentenza del 13 settembre 2018, n. 58170/13 e altri, §§ 249 e seguenti).575 e seguenti>; vedere anche i commenti sullo stato della vittima dei denuncianti e sulla disponibilità di rimedi interni in EGMR, Big Brother Watch e altri v. Regno Unito, sentenza del 13 settembre 2018, n. 58170/13 e altri, §§ 249 e seguenti).

281

d) deve essere garantito il controllo continuo nell'indipendenza istituzionale. Ciò include un bilancio assegnato alle autorità di vigilanza e - a parte la nomina dei membri dell'organo giudiziario e il livello di gestione - la sovranità del personale. Nel loro lavoro, le autorità di vigilanza devono essere efficacemente protette da fattori di influenza e devono pertanto essere completamente indipendenti.

282

Inoltre, il legislatore ha molta latitudine nella questione del disegno istituzionale degli organi di controllo. Ciò riguarda, ad esempio, la questione se il controllo amministrativo amministrativo debba essere garantito dal responsabile federale della protezione dei dati o da un'autorità di controllo indipendente. Tuttavia, il legislatore dovrà organizzare il controllo in modo tale da non essere ostacolato dalla "regola di terzi" (sotto il margine 292 ss.). Inoltre, non esiste un requisito costituzionale per stabilire se il controllo giudiziario e il controllo giuridico amministrativo siano riuniti istituzionalmente sotto lo stesso tetto, in modo tale che gli organi decisionali giudiziari siano integrati in un organo di vigilanza globale, pur mantenendo l'indipendenza giudiziaria dei loro membri.o se dovrebbero essere progettati ciascuno indipendentemente. Tuttavia, è necessario creare strutture istituzionalmente chiare.

283

e) Nel complesso, l'equipaggiamento delle autorità di controllo deve essere orientato verso un'adempimento efficace e indipendente dei loro compiti.

284

aa) Le autorità di controllo devono essere competenti, professionalmente attrezzate ed equilibrate. Anche i legislatori dispongono di una vasta gamma di opzioni al riguardo. Tuttavia, è obbligato a basare il suo progetto sulla garanzia di un controllo efficace, giuridicamente e effettivamente indipendente.

285

(1) A questo proposito, sono richiesti regolamenti che richiedono una nomina di persone che sono specificamente qualificate e qualificate per penetrare nei processi dell'autorità e garantire un controllo indipendente e professionalmente competente nell'interazione reciproca. In ogni caso, il controllo amministrativo non dovrebbe richiedere solo la considerazione delle persone con conoscenze legali, ma anche di altro tipo, in particolare delle tecnologie informatiche.

286

(2) Per il controllo giudiziario, deve essere garantita l'indipendenza dei membri designati per la decisione, che equivale all'indipendenza giudiziaria. In particolare, devono essere privi di istruzioni ed essere nominati per un periodo sufficientemente lungo e specifico. Per la composizione dell'organismo di aggiudicazione, è necessario garantire che la prospettiva giudiziaria abbia un peso significativo, che per un numero significativo di membri deve essere comprovata da molti anni di esperienza giudiziaria. Ciò non preclude la presa in considerazione dell'esperienza acquisita in altre professioni legali. Va anche tenuto presente che altre competenze, in particolare tecniche, possono essere utili. Spetta al legislatore deciderese prevede anche che i non avvocati siano membri

dell'organo decisionale di tipo giudiziario - a seconda del tipo di decisione - in determinate circostanze, o se offre al comitato altre opzioni per avvalersi delle competenze tecniche.

287

(3) Complessivamente, le persone che lavorano a tempo pieno devono garantire un controllo tecnicamente competente e professionale; non è sufficiente basare l'attuazione del controllo essenzialmente su una funzione volontaria. Allo stesso tempo, è necessario prestare attenzione per garantire una composizione equilibrata degli organi di controllo. In termini di personale e struttura, al fine di garantire la necessaria indipendenza, occorre fare attenzione a mantenere una distanza sufficiente dal Servizio di intelligence federale.

288

bb) È necessario fornire personale e risorse adeguati per entrambi i tipi di controllo. Per il controllo da parte del tribunale, è richiesto un numero sufficiente di posti e pannelli, il che consente di svolgere i compiti di controllo da assegnare loro con cura; le posizioni devono essere equipaggiate finanziariamente in modo tale da mettere in evidenza persone qualificate. Il controllo legale amministrativo richiede anche un numero sufficiente di posizioni per dipendenti qualificati. Le risorse materiali devono avere un ambito che consenta, ad esempio, anche di controllare efficacemente i processi di filtraggio per separare la comunicazione tra tedeschi e tedeschi e per proteggere le relazioni di riservatezza e, se necessario, sviluppare i propri file e programmi di controllo a tale scopo.In ogni caso, è improbabile che la portata delle posizioni e dei fondi da creare a tale riguardo sia inferiore a quella attualmente assegnata al rappresentante permanente dell'organismo di controllo parlamentare.

289

f) Le autorità di controllo devono disporre di tutti i poteri necessari per un controllo efficace nei confronti del Servizio di intelligence federale.

290

aa) Ad entrambi gli organi di controllo deve essere garantito un accesso completo a tutti i documenti. Il Servizio federale di informazione è tenuto a sostenere le autorità di vigilanza nell'adempimento dei loro compiti, a fornire loro informazioni e ad ispezionare documenti e dati, a fornire informazioni sui programmi utilizzati e ad accedere ai locali di servizio in qualsiasi momento (vedere BVerfGE 133, 277 <370 f. Marg 215 ss.>; 141, 220 <284 f. Marginale 141>; vedere anche BTDrucks 14/5655, p. 26 con riferimento a BVerfGE 100, 313 <401>). Gli organi di controllo sono responsabili della determinazione della loro procedura e della scelta dei loro metodi, a meno che non siano previsti dalla legge.

291

bb) I requisiti costituzionali in materia di controllo comprendono l'elaborazione dei dati di registrazione (vedere BVerfGE 133, 277 <370 marginale 215>; 141, 220 <284 f marginale 141>; stRspr). Successivamente, è necessario registrare le diverse fasi del monitoraggio in modo da consentire un controllo efficace. Se necessario, i principi pertinenti dovrebbero essere specificati più dettagliatamente nel comportamento tra il servizio di intelligence federale e le autorità di controllo.

292

cc) Il controllo non può essere ostacolato con riferimento alla "Regola di terze parti". Il legislatore deve creare le condizioni in modo tale che la "Regola di terzi" non possa essere contrastata dalle autorità di controllo mediante la progettazione delle autorità di controllo, nonché mediante accordi corrispondenti del Servizio federale di intelligence con gli altri servizi.

293

Tuttavia, la "Regola di terze parti" è un codice di condotta generalmente riconosciuto basato su accordi con servizi dei partner, in base al quale le informazioni provenienti da servizi stranieri non possono essere trasmesse a terzi senza il loro consenso in conformità con accordi informali (vedere BVerfGE 143, 101 <150 marg 162; 151 marginale 164>). Anche il governo federale può fare affidamento su questa regola, a condizione che abbia dato le opportune promesse, sulla base delle quali le informazioni sono già state trasmesse dal servizio estero e dopo di che una trasmissione a "terzi" è quindi in questione;In questo senso, il governo federale ha potuto fare affidamento su impegni assunti con gli Stati Uniti d'America e ha trattenuto alcune informazioni da un comitato investigativo del Bundestag tedesco come terza parte (cfr. VerfGE 143, 101 <152 para 167; 155 ss. Par. 176 ss. .>).

294

Tuttavia, ciò non può essere tenuto contro il controllo legale costituzionale e completo nei confronti del Servizio di intelligence federale sotto forma di organismi indipendenti strettamente confidenziali e impegnati che non sono coinvolti nel parlamento e nei suoi contesti di comunicazione politica. Non è generalmente definito se un'autorità di controllo debba essere considerata come una "terza parte" nel senso di "regola della terza parte", ma dipende dalla struttura organizzativa e dai relativi accordi (cfr. BTDrucks 18/12850, p. 98 f.). A questo proposito, la "Regola di terze parti" è una pratica amministrativa che si basa su una norma giuridicamente non vincolante, ma basata su un accordo con altri servizi, e quindi flessibile, l'importanza pratica di cui il governo federale ha influenza (cfr. Gärditz,DVBl 2015, p. 903 <904 f.>; Möllers, JZ 2017, p. 271 <277>). Il governo federale e il servizio di intelligence federale restano vincolati agli impegni. Per il futuro, tuttavia, la natura del design degli organismi di controllo e i cambiamenti negli accordi con i servizi esteri creeranno le condizioni affinché gli organismi incaricati del controllo legale non possano più essere considerati "terzi" (cfr. Anche Commissione europea per la democrazia attraverso Legge [Commissione di Venezia], Rapporto sulla supervisione democratica delle agenzie di intelligence dei segnali, CDL-AD [2015] 011, p. 5 [n. 13]; Consiglio d'Europa, Assemblea parlamentare, risoluzione 1838 [2011], p. 2 [Punto 7]; Consiglio d'Europa, Commissario per i diritti umani, controllo democratico ed efficace dei servizi di sicurezza nazionale, 2015, p. 13 [Raccomandazione n. 16]).P. 903 <904 f.>; Möllers, JZ 2017, p. 271 <277>). Il governo federale e il servizio di intelligence federale restano vincolati agli impegni. Per il futuro, tuttavia, la natura del design degli organismi di controllo e i cambiamenti negli accordi con i servizi esteri creeranno le condizioni affinché gli organismi incaricati del controllo legale non possano più essere considerati "terzi" (cfr. Anche Commissione europea per la democrazia attraverso Legge [Commissione di Venezia], Rapporto sulla supervisione democratica delle agenzie di intelligence dei segnali, CDL-AD [2015] 011, p. 5 [n. 13]; Consiglio d'Europa, Assemblea parlamentare, risoluzione 1838 [2011], p. 2 [Punto 7]; Consiglio d'Europa, Commissario per i diritti umani, controllo democratico ed efficace dei servizi di sicurezza nazionale, 2015, p. 13 [Raccomandazione n. 16]).P. 903 <904 f.>; Möllers, JZ 2017, p. 271 <277>). Il governo federale e il servizio di intelligence federale restano vincolati agli impegni. Per il futuro, tuttavia, la natura del design degli organismi di controllo e i cambiamenti negli accordi con i servizi esteri creeranno le condizioni affinché gli organismi incaricati del controllo legale non possano più essere considerati "terzi" (cfr. Anche Commissione europea per la democrazia attraverso Legge [Commissione di Venezia], Rapporto sulla supervisione

democratica delle agenzie di intelligence dei segnali, CDL-AD [2015] 011, p. 5 [n. 13]; Consiglio d'Europa, Assemblea parlamentare, risoluzione 1838 [2011], p. 2 [Punto 7]; Consiglio d'Europa, Commissario per i diritti umani, controllo democratico ed efficace dei servizi di sicurezza nazionale, 2015, p. 13 [Raccomandazione n. 16]).904 f.>; Möllers, JZ 2017, p. 271 <277>). Il governo federale e il servizio di intelligence federale restano vincolati agli impegni. Per il futuro, tuttavia, la natura del design degli organismi di controllo e i cambiamenti negli accordi con i servizi esteri creeranno le condizioni affinché gli organismi incaricati del controllo legale non possano più essere considerati "terzi" (cfr. Anche Commissione europea per la democrazia attraverso Legge [Commissione di Venezia], Rapporto sulla supervisione democratica delle agenzie di intelligence dei segnali, CDL-AD [2015] 011, p. 5 [n. 13]; Consiglio d'Europa, Assemblea parlamentare, risoluzione 1838 [2011], p. 2 [Punto 7]; Consiglio d'Europa, Commissario per i diritti umani, controllo democratico ed efficace dei servizi di sicurezza nazionale, 2015, p. 13 [Raccomandazione n. 16]).904 f.>; Möllers, JZ 2017, p. 271 <277>). Il governo federale e il servizio di intelligence federale restano vincolati agli impegni. In futuro, tuttavia, la natura del design degli organismi di controllo e i cambiamenti negli accordi con i servizi stranieri creeranno le condizioni affinché gli organismi incaricati del controllo legale non possano più essere considerati "terzi" (cfr. Anche Commissione europea per la democrazia attraverso Legge [Commissione di Venezia], Rapporto sulla supervisione democratica delle agenzie di intelligence dei segnali, CDL-AD [2015] 011, p. 5 [n. 13]; Consiglio d'Europa, Assemblea parlamentare, risoluzione 1838 [2011], p. 2 [Punto 7]; Consiglio d'Europa, Commissario per i diritti umani, controllo democratico ed efficace dei servizi di sicurezza nazionale, 2015, p. 13 [Raccomandazione n. 16]).P. 271 <277>). Il governo federale e il servizio di intelligence federale restano vincolati agli impegni. In futuro, tuttavia, la natura del design degli organismi di controllo e i cambiamenti negli accordi con i servizi stranieri creeranno le condizioni affinché gli organismi incaricati del controllo legale non possano più essere considerati "terzi" (cfr. Anche Commissione europea per la democrazia attraverso Legge [Commissione di Venezia], Rapporto sulla supervisione democratica delle agenzie di intelligence dei segnali, CDL-AD [2015] 011, p. 5 [n. 13]; Consiglio d'Europa, Assemblea parlamentare, risoluzione 1838 [2011], p. 2 [Punto 7]; Consiglio d'Europa, Commissario per i diritti umani, controllo democratico ed efficace dei servizi di sicurezza nazionale, 2015, p. 13 [Raccomandazione n. 16]).P. 271 <277>). Il governo federale e il servizio di intelligence federale restano vincolati agli impegni. In futuro, tuttavia, la natura del design degli organismi di controllo e i cambiamenti negli accordi con i servizi stranieri creeranno le condizioni affinché gli organismi incaricati del controllo legale non possano più essere considerati "terzi" (cfr. Anche Commissione europea per la democrazia attraverso Legge [Commissione di Venezia], Rapporto sulla supervisione democratica delle agenzie di intelligence dei segnali, CDL-AD [2015] 011, p. 5 [n. 13]; Consiglio d'Europa, Assemblea parlamentare, risoluzione 1838 [2011], p. 2 [Punto 7]; Consiglio d'Europa, Commissario per i diritti umani, controllo democratico ed efficace dei servizi di sicurezza nazionale, 2015, p. 13 [Raccomandazione n. 16]).Il governo federale e il servizio di intelligence federale restano vincolati agli impegni. In futuro, tuttavia, la natura del design degli organismi di controllo e i cambiamenti negli accordi con i servizi stranieri creeranno le condizioni affinché gli organismi incaricati del controllo legale non possano più essere considerati "terzi" (cfr. Anche Commissione europea per la democrazia attraverso Legge [Commissione di Venezia], Rapporto sulla supervisione democratica delle agenzie di intelligence dei segnali, CDL-AD [2015] 011, p. 5 [n. 13]; Consiglio d'Europa, Assemblea parlamentare, risoluzione 1838 [2011], p. 2 [Punto 7]; Consiglio d'Europa, Commissario per i diritti umani, controllo democratico ed efficace dei servizi di sicurezza nazionale, 2015, p. 13 [Raccomandazione n. 16]).Il governo federale e il servizio di intelligence federale restano vincolati agli impegni. In futuro, tuttavia, la natura del design degli organismi di controllo e i cambiamenti negli accordi con i servizi stranieri creeranno le condizioni affinché gli organismi incaricati del controllo legale non possano più essere considerati "terzi" (cfr. Anche Commissione europea per la democrazia attraverso Legge [Commissione di Venezia], Rapporto sulla supervisione democratica delle agenzie di intelligence dei segnali, CDL-AD [2015] 011, p. 5 [n. 13]; Consiglio d'Europa,

Assemblea parlamentare, risoluzione 1838 [2011], p. 2 [Punto 7]; Consiglio d'Europa, Commissario per i diritti umani, controllo democratico ed efficace dei servizi di sicurezza nazionale, 2015, p. 13 [Raccomandazione n. 16]).In futuro, tuttavia, la natura del design degli organismi di controllo e i cambiamenti negli accordi con i servizi stranieri creeranno le condizioni affinché gli organismi incaricati del controllo legale non possano più essere considerati "terzi" (cfr. Anche Commissione europea per la democrazia attraverso Legge [Commissione di Venezia], Rapporto sulla supervisione democratica delle agenzie di intelligence dei segnali, CDL-AD [2015] 011, p. 5 [n. 13]; Consiglio d'Europa, Assemblea parlamentare, risoluzione 1838 [2011], p. 2 [Punto 7]; Consiglio d'Europa, Commissario per i diritti umani, controllo democratico ed efficace dei servizi di sicurezza nazionale, 2015, p. 13 [Raccomandazione n. 16]).In futuro, tuttavia, la natura del design degli organismi di controllo e i cambiamenti negli accordi con i servizi stranieri creeranno le condizioni affinché gli organismi incaricati del controllo legale non possano più essere considerati "terzi" (cfr. Anche Commissione europea per la democrazia attraverso Legge [Commissione di Venezia], Rapporto sulla supervisione democratica delle agenzie di intelligence dei segnali, CDL-AD [2015] 011, p. 5 [n. 13]; Consiglio d'Europa, Assemblea parlamentare, risoluzione 1838 [2011], p. 2 [Punto 7]; Consiglio d'Europa, Commissario per i diritti umani, controllo democratico ed efficace dei servizi di sicurezza nazionale, 2015, p. 13 [Raccomandazione n. 16]).che gli organi responsabili del controllo legale non sono più considerati "soggetti terzi" (cfr. anche Commissione europea per la democrazia attraverso il diritto [Commissione di Venezia], Rapporto sulla supervisione democratica delle agenzie di intelligence dei segnali, CDL-AD [2015] 011, p. 5 [n. 13]; Consiglio d'Europa, Assemblea parlamentare, Risoluzione 1838 [2011], p. 2 [voce 7]; Consiglio d'Europa, Commissario per i diritti umani, controllo democratico ed efficace dei servizi di sicurezza nazionale, 2015, p. 13 [Raccomandazione n. 16]).che gli organi responsabili del controllo legale non sono più considerati "soggetti terzi" (cfr. anche Commissione europea per la democrazia attraverso il diritto [Commissione di Venezia], Rapporto sulla supervisione democratica delle agenzie di intelligence dei segnali, CDL-AD [2015] 011, p. 5 [n. 13]; Consiglio d'Europa, Assemblea parlamentare, Risoluzione 1838 [2011], p. 2 [voce 7]; Consiglio d'Europa, Commissario per i diritti umani, controllo democratico ed efficace dei servizi di sicurezza nazionale, 2015, p. 13 [Raccomandazione n. 16]).Consiglio d'Europa, Commissario per i diritti umani, controllo democratico ed efficace dei servizi di sicurezza nazionale, 2015, p. 13 [Raccomandazione n. 16]).Consiglio d'Europa, Commissario per i diritti umani, controllo democratico ed efficace dei servizi di sicurezza nazionale, 2015, p. 13 [Raccomandazione n. 16]).

295

In questo modo si deve garantire che sia l'attività di controllo costituzionalmente richiesta si estenda senza ostacoli dalla "Regola di terzi" al trattamento delle informazioni da parte del Servizio di intelligence federale da servizi stranieri, sia quello per la protezione degli interessi di politica estera e di sicurezza della Repubblica Federale in particolare si può continuare una significativa cooperazione tra il Servizio di intelligence federale e altri servizi di intelligence (margine n. 246 f. sopra). Che ciò sia possibile è evidente anche per quanto riguarda altri servizi di intelligence, in cui le autorità di vigilanza hanno pieno accesso a tutti i documenti necessari per il controllo dei servizi che controllano (cfr. Per i diritti di informazione del tribunale per i poteri di indagine nel Regno Unito EGMR, Big Brother Watch e altri c. Regno Unito,Sentenza del 13 settembre 2018, n. 58170/13 e altri, §§ 250, 379; per i diritti di accesso illimitati del Commissario per i poteri di indagine, consultare la relazione annuale del Commissario per i poteri di indagine 2017 del 31 gennaio 2019, pag.41).

296

dd) Il controllo può essere generalmente accompagnato da rigide regole di riservatezza. Oltre alle attrezzature spaziali e tecniche, questo può anche svolgere un ruolo significativo nella selezione delle persone. In particolare, la riservatezza può essere garantita da rigorosi obblighi di riservatezza applicati con sanzioni efficaci.

297

(1) Al contrario, deve essere garantito uno scambio aperto e diretto tra gli organi di vigilanza incaricati del controllo giuridico oggettivo (vedere BVerfGE 133, 277 <370 marginale n. 216>). Dal momento che entrambi - entrambi egualmente impegnati nella riservatezza - lavorano insieme per controllare le stesse misure, ciò richiede un controllo efficace e coerente. Nella misura in cui emergono problemi strutturali nel corso del controllo o se vi sono altre differenze che non possono essere chiarite con il Servizio di intelligence federale, deve essere fornita la possibilità di denunciare eventuali reclami alle autorità e, se necessario, alla direzione della Cancelleria federale di controllo, che potrebbe dover essere correlata a questo.

298

(2) Il flusso di informazioni nell'area parlamentare e quindi anche verso l'organo di controllo parlamentare può tuttavia essere limitato per motivi di riservatezza. A tale proposito, il legislatore può tener conto del fatto che il controllo parlamentare ha un carattere diverso (inferiore ai 300 marginali) rispetto a un controllo che è esclusivamente orientato all'osservanza della legge oggettiva e che la riservatezza nell'ambiente parlamentare-politico è soggetta a limiti di fatto. Tuttavia, l'organismo di controllo parlamentare ai sensi dell'articolo 45 quinquies GG in una forma, che tiene conto degli interessi della protezione segreta, deve essere regolarmente informato sull'attività di controllo. Inoltre, le autorità di vigilanza devono essere in grado di utilizzare abstract,la segretezza garantisce che le sue denunce e critiche vengano in definitiva trasmesse al Parlamento e quindi al pubblico.

299

(3) Poiché i processi di controllo del parlamento e del pubblico rimangono in gran parte chiusi, ma allo stesso tempo esiste una potenziale tensione tra il lavoro del Servizio di intelligence federale basato sul principio di segretezza e, inoltre, le condizioni delle misure di sorveglianza e il loro controllo possono cambiare rapidamente in vista dell'ulteriore sviluppo della tecnologia , l'efficacia del controllo richiede un'osservazione costante. L'efficacia sia del controllo in pratica che delle norme legali deve essere valutata ad intervalli regolari (per gli obblighi di valutazione si veda anche BVerfGE 150, 1 <90 marginale n. 176>).

300

g) L'attuale controllo da parte dell'organismo di controllo parlamentare e del suo rappresentante permanente, anch'esso soggetto al legislatore e che può essere incluso nel controllo delle misure di monitoraggio (cfr. ad es. § 14 G 10), non è oggetto del presente procedimento. Ha una sua funzione, che non è specificamente limitata al controllo legale e dei diritti fondamentali ed è un'espressione della responsabilità parlamentare generale per la corretta e politicamente adeguata esecuzione dei compiti dell'esecutivo (cfr. Waldhoff, in: Dietrich / Gärditz / Graulich / Gusy / Warg [Ed.], Riforma dei servizi di intelligence tra legalizzazione e internazionalizzazione, 2019, p. 73 <75>).I requisiti per la loro progettazione non possono essere derivati dai diritti fondamentali rivendicati nel presente procedimento; Viceversa, a questo proposito, i poteri del Parlamento sull'esecutivo che

derivano dalla costituzione rimangono inalterati dalle disposizioni di cui sopra (cfr. BVerfGE 143, 101).

VI.

301

Secondo le disposizioni di cui sopra, anche i regolamenti impugnati non soddisfano materialmente i requisiti costituzionali. Come la violazione dell'obbligo di citazione dell'articolo 19.1 frase 2 della Legge fondamentale (paragrafo 134 f. Sopra), si basano sul presupposto costituzionalmente errato che i diritti fondamentali non sono applicabili ai poteri di vigilanza in questione. Poiché i regolamenti sono incostituzionali per motivi formali, solo i disavanzi centrali vengono affrontati nella loro valutazione materiale. Un nuovo regolamento sui poteri del Servizio di intelligence federale dovrà inoltre allineare i regolamenti nel loro insieme ai diritti fondamentali delle persone monitorate in relazione alle loro telecomunicazioni e quindi ai requisiti sviluppati sopra.

302

1. Le disposizioni relative alla raccolta e al trattamento dei dati di cui alle sezioni 6, 7 BNDG sono inizialmente incompatibili con l'articolo 10 capoverso 1 GG e i conseguenti requisiti di proporzionalità.

303

a) Ciò vale da un lato per la regolamentazione della sorveglianza strategica dall'interno della Germania, conformemente alla sezione 6 BNDG.

304

aa) La Sezione 6 BNDG non disciplina la violazione dei diritti fondamentali contro tedeschi e residenti attualmente inevitabili per motivi tecnici, che attualmente è inevitabile nella maniera costituzionale. In particolare, non regola in modo sufficiente il filtraggio richiesto a questo proposito e i requisiti che devono essere soddisfatti da questo filtraggio (margine n. 170 ss. Sopra). Il divieto materiale nella sola sezione 6 (4) del BNDG, che fa sembrare che i dati dei cittadini e dei cittadini tedeschi nel loro insieme debbano e possano essere evitati, non è sufficiente. La cancellazione immediata richiesta della comunicazione domestica registrata inavvertitamente non è regolata secondo le norme. La sezione 10 (4) frase 1 BNDG prevede sostanzialmente tale cancellazione.La norma non dice se e fino a che punto tale cancellazione possa essere revocata secondo le frasi da 2 a 6 del regolamento (vedi Hölscheidt, Jura 2017, p. 148 <156>).

305

bb) Inoltre, la sorveglianza secondo la Sezione 6 BNDG non si limita a scopi differenziati e pesanti (sopra il margine 175 f.). Le finalità ampiamente e apertamente formulate menzionate nella Sezione 6, paragrafo 1, frase 1, BNDG, che non dovrebbero restringere la gamma di compiti in alcun modo anche dopo che il disegno di legge era giustificato (cfr. BTDrucks 18/9041, p. 22), non soddisfano chiaramente questo requisito. In particolare, tale limitazione legale non può essere sostituita dall'unico mandato politicamente definito del governo federale (cfr. Ufficio delle Nazioni Unite dell'Alto commissario per i diritti umani, lettera del relatore speciale datata 29 agosto 2016, OL DEU 2/2016 , P. 5).

306

Di conseguenza, la sorveglianza non è strutturata sulla base di disposizioni formalizzate di misure di sorveglianza differenziate, in base alle quali la selezione dei percorsi di trasmissione da registrare, nonché i termini di ricerca, nonché l'ulteriore elaborazione e utilizzo devono essere verificabili in modo verificabile sul principio di proporzionalità (cfr. Margine n. 178 ss.; Cfr. in generale anche Marxsen, DÖV 2018, p. 218 <224>). Vi è anche una mancanza di requisiti legali per l'uso di termini di ricerca personale mirati (margine n. 185 ss. Sopra) e per la protezione delle relazioni di riservatezza (margine n. 193 ss. Sopra e Löffelmann, in: Dietrich / Gärditz / Graulich / Gusy / Warg [ed.], Riforma dei servizi di intelligence tra legalizzazione e internazionalizzazione, 2019, p. 33 <43>).La protezione dell'area centrale in § 11 BNDG è insufficientemente regolata (margine 203 ss. Sopra).

307

Allo stesso modo, la legge non contiene regolamenti sufficienti per la valutazione dei dati ottenuti mediante intelligence strategica straniera (sopra, punto 192). Sezione 19 BNDG, come regola generale per l'elaborazione dei dati da parte del Servizio federale di intelligence, non soddisfa questi requisiti ed è nel suo ambito non specifico e il riferimento indifferenziato alle sezioni 10 e 11 BVerfSchG come base per l'elaborazione, la modifica e l'uso dei dati basati su §§ 6, 7 BNDG sono stati sollevati, sproporzionati.

308

cc) Nella misura in cui § 6 BNDG dovrebbe anche fungere da base per la raccolta di altri dati personali di cittadini tedeschi, persone giuridiche nazionali o persone residenti nel territorio federale che non sono soggetti all'articolo 10 GG (cfr. BTDrucks 18/9041, p. 24) , il regolamento manca già della necessaria chiarezza delle norme (cfr. margine n. 137 e seguenti). Dal regolamento non risulta già che l'uso di tali dati non protetti dal segreto delle telecomunicazioni dovrebbe essere aperto da loro; Tanto più che non regola quali dati dovrebbero essere raccolti per quale uso e su quale base questi siano considerati giustificati dal legislatore in merito a quali diritti fondamentali.

309

b) In secondo luogo, l'articolo 7 BNDG, che regola l'ulteriore trattamento dei dati ottenuti dall'estero attraverso l'educazione alle telecomunicazioni e alcuni limiti di tale raccolta di dati, non è compatibile con l'articolo 10, paragrafo 1, GG. Il regolamento si basa sul presupposto errato che tale raccolta di dati non richiede una base di autorizzazione ed è possibile solo sulla base dello standard di attività di cui alla Sezione 1 (2) BNDG. Senza un'autorizzazione legale sufficiente, tuttavia, tale raccolta di dati è anche inammissibile (paragrafi 87 e seguenti e 120 supra). Dal momento che § 7 BNDG implica l'ammissibilità di questa raccolta di dati, la limita solo in modo selettivo e altrimenti consente un ulteriore trattamento senza ulteriori indugi, è essa stessa incostituzionale.Come sua (implicita) autorizzazione a raccogliere dati, non ha soddisfatto i requisiti costituzionali sopra indicati per tale base giuridica. Come visto, il legislatore non vuole che § 7 BNDG sia inteso come base per autorizzare la raccolta di dati. Quindi § 7 BNDG viola già l'articolo 10 capoverso 1 GG in quanto regola il trattamento dei dati che non sarebbero stati raccolti a causa della mancanza di una base giuridica costituzionale e quindi non avrebbero dovuto essere ulteriormente trattati. Inoltre, dà l'impressione che tali dati possano essere raccolti e quindi legittima una raccolta di dati per la quale non esiste una base giuridica costituzionale.non comprendere affatto come base di autorizzazione per la raccolta dei dati. Quindi § 7 BNDG viola già l'articolo 10 capoverso 1 GG in quanto regola il trattamento dei dati che non sarebbero stati raccolti a causa della

mancanza di una base giuridica costituzionale e quindi non avrebbero dovuto essere ulteriormente trattati. Inoltre, dà l'impressione che tali dati possano essere raccolti e quindi legittima una raccolta di dati per la quale non esiste una base giuridica costituzionale.non comprendere affatto come base di autorizzazione per la raccolta dei dati. Quindi § 7 BNDG viola già l'articolo 10 capoverso 1 GG in quanto regola il trattamento dei dati che non sarebbero stati raccolti a causa della mancanza di una base giuridica costituzionale e quindi non avrebbero dovuto essere ulteriormente trattati. Inoltre, dà l'impressione che tali dati possano essere raccolti e quindi legittima una raccolta di dati per la quale non esiste una base giuridica costituzionale.che tali dati possano essere raccolti e quindi legittimare la raccolta di dati per i quali non esiste una base giuridica costituzionale.che tali dati possano essere raccolti e quindi legittimare la raccolta di dati per i quali non esiste una base giuridica costituzionale.

310

2. Anche le norme sulla trasmissione dei dati non sono compatibili con i requisiti costituzionali. Alcuni di essi non soddisfano il principio di chiarezza delle norme. Inoltre, non limitano sufficientemente la trasmissione alla protezione di interessi legali particolarmente importanti o il perseguimento di reati particolarmente gravi, né li vincolano a una situazione di rischio sufficientemente specifica o al sospetto di tali crimini comprovati da determinati fatti.

311

a) Sezione 24 (1) frase 1 BNDG, che regola la trasmissione a enti pubblici nazionali, non soddisfa i requisiti di chiarezza delle norme e della certezza (paragrafi 137 e seguenti e 212 e seguenti). Ciò si applica inizialmente nella misura in cui generalmente consente al Servizio di intelligence federale di trasmettere "per svolgere i propri compiti". Un riferimento a compiti definiti altrove non è sostanzialmente incompatibile con i requisiti di chiarezza delle norme. Un riferimento generale a tutti i compiti del Servizio di intelligence federale, che non include alcuna attività operativa, ma si limita esclusivamente all'acquisizione di conoscenze e alla sua valutazione (cfr. § 1 comma 2 BNDG), non indica tuttavia gli scopi per i quali la trasmissione dei dati qui dovrebbe essere consentito (paragrafo 215 sopra).Ciò è stato confermato dalle incertezze in udienza. Tuttavia, il regolamento è anche indefinito in quanto consente la trasmissione se il destinatario ha bisogno dei dati per scopi significativi di pubblica sicurezza. Dal momento che non è chiaro se ciò si riferisca a tutte le autorità coinvolte nell'applicazione della legge generale o eventualmente anche normativa speciale o solo delle autorità di sicurezza specifiche, non lo chiarisce al gruppo di autorità destinatarie. Per il resto, mancano i requisiti sia per quanto riguarda le soglie di intervento necessarie sia per quanto riguarda una protezione qualificata degli interessi legali per entrambi gli articoli di trasmissione (si veda in ogni caso il margine n. 220 e seguenti). Il riferimento indefinito a scopi "significativi" di pubblica sicurezza,che dovrebbe escludere solo fatti banali (cfr. la formulazione della stessa formulazione nella Sezione 19 (1) frase 2 BVerfSchG BTDrucks 18/4654, p. 34) non è sufficiente per questo.

312

b) Sezione 24 (3) BNDG in combinato disposto con la Sezione 20 (1) frasi 1 e 2 BVerfSchG, che autorizza la trasmissione di informazioni nel contesto di reati di sicurezza dello stato alla polizia e ai pubblici ministeri, non è compatibile con i requisiti costituzionali. Le autorità riceventi sono certamente sufficientemente determinate qui. Tuttavia, è discutibile se la catena di riferimenti multi-link soddisfi ancora i requisiti di chiarezza delle norme (margine n. 215 sopra). Indipendentemente da ciò, i requisiti per la tutela degli interessi legali non sono sempre soddisfatti al riguardo (sopra, nm. 221). Perché non tutti i reati menzionati nelle Sezioni 74a, 120 GVG e generalmente indicati

dal regolamento possono essere classificati come reati particolarmente gravi. Lo stesso vale per il fatto aperto di trasmissione,che include qualsiasi altro reato basato esclusivamente sui loro obiettivi o sul motivo dell'autore. Inoltre, la disposizione non determina adeguatamente la soglia di trasmissione richiesta (paragrafi 213 e seguenti, 220 e seguenti e 227 e seguenti). A questo proposito, il legislatore deve formulare requisiti che devono soddisfare i requisiti per una specifica situazione di rischio (cfr. BVerfGE 141, 220 <271 ss. Margine 111 ss.>) O fatti che forniscono sufficienti motivi di sospetto.>) o deve corrispondere a fatti che suscitano sospetti.>) o deve corrispondere a fatti che suscitano sospetti.

313

c) Anche la Sezione 24 Paragrafo 2 Frase 1 BNDG in combinato disposto con la Sezione 19 Paragrafo 4 BVerfSchG, che regola un trasferimento ad "altri" - e quindi essenzialmente organismi privati - non soddisfa i requisiti dell'articolo 10, paragrafo 1 GG in tutti i sensi. Tuttavia, la disposizione non può essere contestata né dal punto di vista della certezza né in termini di tutela giuridica richiesta con essa. Il riferimento alla "protezione del libero ordine democratico di base, l'esistenza o la sicurezza del governo federale o di uno stato", nonché al "garantire la sicurezza delle strutture vitali o legate alla difesa ai sensi del § 1 paragrafo 4 della legge sull'ispezione di sicurezza" è nel contesto dell'altra ha introdotto chiaramente la comprensione del termine e nomina i prodotti legali di peso particolarmente elevato. Tuttavia, è di nuovo discutibilese il riferimento multilivello è sufficiente per la chiarezza degli standard (vedere il margine n. 213 ss. sopra). In ogni caso, non esiste una soglia di trasmissione (paragrafi 216 e seguenti e 222 sopra).

314

d) Anche incostituzionale è la Sezione 24 (2) frase 1 BNDG in combinato disposto con la Sezione 19 (2) BVerfSchG, che - con riferimento all'articolo 3 dell'accordo aggiuntivo all'accordo tra le parti del Trattato del Nord Atlantico sullo status giuridico delle loro truppe in relazione al Truppe straniere di stanza nella Repubblica Federale Tedesca (Accordo aggiuntivo sullo statuto delle truppe della NATO) del 3 agosto 1959 (BGBl 1961 II p. 1218) - è consentita la trasmissione di informazioni alle forze di stazionamento della NATO. La disposizione inizialmente manca della chiarezza e certezza richieste (sopra, punti 137 e seguenti e 213 e seguenti). Il riferimento tripartito a una norma di diritto internazionale dei contratti, che a sua volta regola in modo ampio e aperto un quadro generale di cooperazione, non mostra più sufficientemente chiaramente e con certezza cheper quale motivo le informazioni possono essere trasmesse qui. Inoltre, la disposizione non limita la trasmissione a una protezione sufficientemente importante degli interessi legali e non presuppone soglie di trasmissione (in ogni caso margine 220 ss. Sopra). L'impegno per la "necessità" della trasmissione non è sufficiente per questo.

315

e) Infine, la sezione 24 (2) frase 1 BNDG in combinato disposto con la sezione 19 (3) BVerfSchG, che regola il trasferimento a enti pubblici stranieri, non soddisfa i requisiti costituzionali sotto vari aspetti.

316

Inizialmente, manca una determinazione sufficientemente precisa delle autorità beneficiarie, che nel presente caso non può essere determinata dagli scopi di trasmissione aperti (sopra, punti 137 e seguenti e 213 e seguenti; cfr. BVerfGE 130, 151 <203>; 133, 277 <337 f. marginale 143>; 141, 220 <334 marginale 306>). Inoltre, la trasmissione non è ancora limitata a interessi legali

adeguatamente qualificati e non viene specificata una soglia di trasmissione (in ogni caso margine 220 ss. Sopra).

317

Allo stesso modo, il regolamento non obbliga il Servizio di intelligence federale in un modo che sia chiaro in termini di standard a garantire che i dati trasmessi siano gestiti in conformità con lo stato di diritto. Gli approcci per questo possono essere trovati nella Sezione 19 (3) frase 2 BVerfSchG. Tuttavia, ciò non soddisfa i requisiti stabiliti in scala (note a margine 233 e seguenti). Ad esempio, non esiste già alcun riferimento esplicito all'assicurazione delle garanzie minime di protezione dei dati (sopra, marginale 235 ss.) E un obbligo di registrazione (sopra il marginale 229). Inoltre, la protezione delle relazioni di riservatezza, ad esempio, non viene presa specificamente in considerazione (margine 240 sopra con margine 193 ss.).

318

L'assicurazione richiesta non è inoltre adeguatamente assicurata dalla Sezione 31 BNDG in combinato disposto con la Sezione 23 n. 1 BVerfSchG: da ciò non si può vedere che l'autorità di trasmissione è attiva riguardo alle circostanze nel paese di destinazione - sia per quanto riguarda la speciale protezione dei dati sia le garanzie sui diritti umani - assicurarsi che ciò sia documentato e che sorgano dubbi (vedere il margine n. 233 ss. sopra). Inoltre, la disposizione non esclude la possibilità di sopprimere le questioni elementari dello Stato di diritto a titolo di valutazione (paragrafo 237 supra).

319

f) Complessivamente, i regolamenti di trasmissione, che si basano prevalentemente sulle strutture della legge sulla protezione costituzionale federale e su altre leggi sulla sicurezza, che sono più vecchi nella loro versione e non sufficientemente adattati allo sviluppo della giurisprudenza, non soddisfano i requisiti costituzionali. Da un punto di vista formale, non vi è inoltre alcun obbligo di registrare la trasmissione (paragrafo 229 sopra) e di indicare la base giuridica utilizzata per la trasmissione (paragrafo 229 sopra) per tutti gli articoli della trasmissione.

320

3. Anche la regolamentazione della cooperazione ai sensi dei §§ 13-15 BNDG non è conforme ai requisiti di proporzionalità di cui all'articolo 10 capoverso 1 GG ed è quindi non solo formalmente ma anche materialmente incostituzionale.

321

a) In primo luogo, continuano i deficit costituzionali che si applicano già alla Sezione 6 BNDG. Mancano anche regole sufficientemente chiare per la separazione dei dati di telecomunicazione dai tedeschi e dai residenti per la raccolta e l'elaborazione dei dati nel quadro di accordi di cooperazione (margine n. 176 ss. E 253 sopra). Allo stesso modo, anche le misure di sorveglianza cooperativa non si limitano a scopi legalmente sufficientemente definiti e importanti (sopra, marg. 175 f. E 253); Sezione 13 (4) BNDG non svolge adeguatamente tale funzione limitante. Di conseguenza, la cooperazione non è impegnata e strutturata da specifici obiettivi di conoscenza da concretizzare (sopra, marginale 178 e seguenti. E 253).

322

b) Nella misura in cui la Sezione 14 (1) BNDG consente la valutazione dei dati raccolti dal Servizio federale di intelligence utilizzando i termini di ricerca specificati dai servizi esteri, ciò non è affiancato da sufficienti obblighi di controllo. In particolare, non vi sono garanzie per le persone particolarmente bisognose di relazioni di protezione e riservatezza (marginali 194 e seguenti e 257 sopra). Per inciso, è materialmente sufficiente che i termini di ricerca rimangano all'interno degli obiettivi di cooperazione, offrano protezione contro la registrazione mirata di obiettivi nell'Unione europea e debbano essere compatibili con gli interessi della Repubblica federale di Germania (cfr. § 14, paragrafo 1, clausole 1 e 2 , Paragrafo 2 BNDG). In termini di procedura, tuttavia, esiste anche un obbligo legale a tale riguardocontrollare efficacemente i termini di ricerca nominati esternamente per la loro ammissibilità materiale sulla base di informazioni minime che devono essere verificate per plausibilità da parte dei servizi esteri - e, se necessario, anche a mano - (vedi margine n. 254 ss. sopra).

323

c) Per la trasmissione automatizzata di dati in conformità con la Sezione 15 (1) BNDG, inizialmente non esiste un regolamento sufficientemente sofisticato per separare i dati che sono particolarmente degni di protezione o che provengono da speciali relazioni di riservatezza (sopra, marg. 194 ss. e 257). Allo stesso modo, la legge non impone ai destinatari di assumere impegni per rispettare le disposizioni in materia di riservatezza e non discriminazione o per salvaguardare le soglie di trasmissione di base (al di sopra del margine n. 260). L'impegno generale e astratto di utilizzare i dati in conformità con lo stato di diritto in conformità con la Sezione 13 (3) n. 4 BNDG non è sufficiente per questo. Non è inoltre prevista una garanzia dello stato di diritto nella forma richiesta (sopra, marginale 233 ss. E 261).Infine, il regolamento non contiene alcuna restrizione alla trasmissione di dati sul traffico non selezionati (margine 262 e seguenti).

324

4. Si può anche vedere senza ulteriori indugi che il Federal Intelligence Service Act non ha creato regolamenti sufficienti per controllare i poteri menzionati. La regolamentazione degli obblighi di informazione strettamente limitati nel § 22 BNDG e la mancanza di obblighi di notifica in merito alle misure di sorveglianza all'estero nei confronti degli stranieri non sono discutibili in sé. Tuttavia, al fine di compensare l'apertura dei regolamenti e la protezione giuridica di fatto molto limitata - come mostrato in scala (sopra il margine n. 267 ss.) - è necessario un controllo obiettivo indipendente esteso.Secondo le norme applicabili, ciò non può essere garantito sin dall'inizio dall'organismo indipendente e dal controllo del responsabile federale della protezione dei dati per quanto riguarda i poteri e la struttura organizzativa e istituzionale secondo le modalità previste dalla Costituzione.

VII.

325

I regolamenti sono inoltre incompatibili con la costituzione nella misura in cui autorizzano misure di sorveglianza contro i giornalisti e giustificano quindi gli interventi di cui all'articolo 5, paragrafo 1, frase 2 della legge di base, poiché non tengono adeguatamente conto delle esigenze di protezione specifiche dei giornalisti stranieri indipendenti (cfr. Anche Ufficio delle Nazioni Unite dell'Alto commissario per i diritti umani, lettera del relatore speciale datata 29 agosto 2016, OL DEU 2/2016, p. 5 f.).

F.

326

Indipendentemente dalla misura in cui la Corte costituzionale federale sarebbe responsabile per l'esame nella presente costellazione, contrariamente a quanto sostengono i denuncianti, non vi sono ulteriori requisiti rispetto ai diritti fondamentali dell'Unione europea. Anche se le disposizioni controverse dovrebbero essere viste in parte alla luce dell'articolo 15 della direttiva 2002/58 / CE come attuazione del diritto dell'Unione ai sensi dell'articolo 51, paragrafo 1, clausola 1, GRCh, non esistono già indicazioni concrete e sufficienti che i diritti fondamentali della Legge fondamentale nella presente interpretazione non garantisce il livello di protezione della Carta dei diritti fondamentali dell'Unione europea nella giurisprudenza della Corte di giustizia europea nella causa da stabilire qui (vedi BVerfG, decisione del Primo Senato del 6 novembre 2019 - 1 BvR 16/13 -, marg 67 e seguenti - Diritto all'oblio I).In particolare, tali indicazioni non sorgono in merito al potere di archiviare e valutare i dati sul traffico dalle decisioni della Corte di giustizia europea sulla direttiva sulla conservazione dei dati (sentenza dell'8 aprile 2014, Digital Rights Ireland e Seitlinger et al., C-293/12, C-594 / 12, EU: C: 2014: 238) e sui poteri di conservazione dei dati degli Stati membri (sentenza del 21 dicembre 2016, Tele2 Sverige e Watson et al., C-203/15 e C-698/15, EU: C: 2016: 970). Tali decisioni riguardavano i requisiti per una registrazione nazionale completa di tutti i dati relativi alle connessioni di telecomunicazione, che consentivano profili di personalità quasi completi dei singoli partecipanti alla comunicazione.Ciò differisce fondamentalmente dalla raccolta di un volume limitato di dati sul traffico per la comunicazione internazionale da reti selezionate - che, di norma, non è in grado di acquisire le relazioni di comunicazione complete degli interessati. Non è pertanto evidente che la tutela dei diritti fondamentali ai sensi della Legge fondamentale non garantirebbe il livello di protezione della Carta dei diritti fondamentali dell'Unione europea nel quadro di una protezione dei diritti fondamentali in Europa basata sulla diversità.che la protezione dei diritti fondamentali della Legge fondamentale non garantirebbe il livello di protezione della Carta dei diritti fondamentali dell'Unione europea nel quadro di una protezione dei diritti fondamentali in Europa basata sulla diversità.che la protezione dei diritti fondamentali della Legge fondamentale non garantirebbe il livello di protezione della Carta dei diritti fondamentali dell'Unione europea nel quadro di una protezione dei diritti fondamentali in Europa basata sulla diversità.

G.

IO.

327

Le sezioni 6, 7, da 13 a 15 del BNDG sono quindi incostituzionali. Sezioni 19, 24 Paragrafo 1 Clausola 1, Paragrafo 2 Clausola 1, Paragrafo 3 BNDG sono anche incostituzionali nella misura in cui si riferiscono ai dati raccolti in conformità con i regolamenti di cui sopra. Essi violano i denuncianti da 2) a 8) nei loro diritti fondamentali ai sensi dell'articolo 10.1 della Legge fondamentale e i denuncianti da 2) a 7) nei loro diritti fondamentali ai sensi dell'articolo 5.1 frase 2 della Legge fondamentale. Le sezioni da 9 a 11, 16, 19, 20, 22, 32, 32a BNDG, che non soddisfano adeguatamente i requisiti per un affiancamento proporzionato dei poteri costituzionali dell'incostituzionale, perdono la loro portata.

328

Resta da vedere se il denunciante 1) come persona giuridica domiciliata in uno stato membro dell'Unione Europea abbia anche i suoi diritti fondamentali violati dai regolamenti controversi. Con la decisione sull'incompatibilità delle disposizioni con la Legge fondamentale, che diventa forza

legale secondo la Sezione 31 Paragrafo 2 Frase 2 BVerfGG, ha almeno raggiunto la sua richiesta di protezione legale nella misura che sarebbe possibile sulla base di eventuali diritti fondamentali .

II.

329

La determinazione dell'incostituzionalità delle norme legali porta sostanzialmente alla loro nullità. Tuttavia, la Corte costituzionale federale, come si può vedere dalla Sezione 31 (2) Clausole 2 e 3 BVerfGG, può anche limitarsi a dichiarare uno standard incostituzionale solo incompatibile con la Legge fondamentale (vedere BVerfGE 109, 190 <235>). Rimane quindi una semplice lamentela sull'incostituzionalità senza che sia dichiarata la nullità. La Corte costituzionale federale può allo stesso tempo combinare la dichiarazione di incompatibilità con l'ordine di mantenere la disposizione incostituzionale per un periodo limitato. Ciò viene preso in considerazione se l'invalidità immediata della norma da contestare priverebbe la protezione dei beni in circolazione del bene comune e comporterebbe un equilibrio con i diritti fondamentali in questione,che l'intervento deve essere tollerato per un periodo transitorio (vedi BVerfGE 33, 1 <13>; 33, 303 <347 f.>; 40, 276 <283>; 41, 251 <266 e seguenti>; 51, 268 <290 e seguenti .>; 109, 190 <235 f.>).

330

Questo è il caso qui. I poteri contestati possono anche avere un'importanza a breve termine per la sicurezza della Repubblica federale di Germania e come base per l'azione del governo federale a seconda della situazione politica, soprattutto se si considerano le potenziali dinamiche degli sviluppi minacciosi nelle condizioni della tecnologia dell'informazione. Una dichiarazione di annullamento o una sospensione provvisoria comporterebbe pertanto notevoli rischi. Inoltre, sospendere bruscamente la capacità di lavorare con altri servizi potrebbe potenzialmente danneggiare la fiducia in una collaborazione affidabile a lungo termine. Al contrario,che i poteri contestati possono essere strutturati in modo costituzionalmente valido secondo la loro struttura di base e possono quindi essere migliorati. Si tratta di miglioramenti fondamentali, poiché una nuova versione deve disciplinare tali misure per la prima volta alla luce dell'articolo 10.1 della Legge fondamentale e deve quindi creare confini e controlli in un modo nuovo. In considerazione della grande importanza che il legislatore può attribuire all'intelligence straniera, è necessario tollerare una continuazione temporanea delle disposizioni incostituzionali piuttosto che la loro eliminazione fino a quando non sarà prevedibile un nuovo regolamento.1 GG regola e quindi deve creare confini e controlli secondo lo stato di diritto. In considerazione della grande importanza che il legislatore può attribuire all'intelligence straniera, è necessario tollerare una continuazione temporanea delle disposizioni incostituzionali piuttosto che la loro eliminazione fino a quando non sarà prevedibile un nuovo regolamento.1 GG regola e quindi deve creare confini e controlli secondo lo stato di diritto. Alla luce della grande importanza che il legislatore può attribuire all'intelligence straniera, è necessario tollerare una continuazione temporanea delle disposizioni incostituzionali piuttosto che la loro eliminazione fino a quando non sarà prevedibile un nuovo regolamento.

331

I legislatori devono creare un nuovo regolamento entro il 31 dicembre 2021. L'ordine di continuazione è limitato a questo punto nel tempo.

III.

332

La decisione di pagamento si basa sulla Sezione 34a (2) BVerfGG.

Harbarth	Masing	Paolo
Orso	Britz	Ott
cristiano	Radtke	