

1.6 Diritto comparato e diritto internazionale pubblico

	Germania <i>Bundesamt für Verfassungsschutz (BfV)</i> <i>Bundesnachrichtendienst (BND)</i>
Posizione nell'architettura di sicurezza	<i>BfV:</i> il servizio informazioni interno (unitamente agli uffici dei Länder incaricati della tutela della Costituzione) è subordinato al Ministero dell'interno. <i>BND:</i> il servizio informazioni concernente l'estero è direttamente subordinato al Governo federale. <i>Oltre a questi due servizi, soltanto il Militärischer Abschirmdienst (MAD) ha uno statuto di servizio informazioni.</i>
Compiti	<i>BfV:</i> - raccogliere e valutare notizie, informazioni e documenti relativi a mene contro l'ordinamento fondamentale liberale e democratico oppure contro la stabilità o la sicurezza della Repubblica federale o di un Land, oppure mene che mediante l'uso della forza o atti preparatori orientati a tal fine minacciano gli interessi esterni della Repubblica federale o contro il principio della comprensione tra i popoli, segnatamente contro la convivenza pacifica dei popoli; - controspionaggio; controproliferazione; protezione dell'economia; collaborazione nell'ambito dei controlli di sicurezza relativi alle persone per la tutela del segreto e la protezione da sabotaggi. <i>BND:</i> - raccogliere e valutare le informazioni necessarie per acquisire conoscenze sull'estero rilevanti per lo Stato in materia di politica estera e di politica di sicurezza; - fornire informazioni politiche, economiche, militari e scientifico-tecnologiche sull'estero.
Competenze (impiego di mezzi di intelligence)	<i>BfV:</i> l'impiego di mezzi di intelligence da parte del BfV è disciplinato nella legislazione. Per adempiere i propri compiti, nel rispetto degli oneri legali al BfV è consentito: - impiegare metodi, oggetti e mezzi per acquisire segretamente informazioni (per es. informatori, osservazioni, registrazioni di immagini e suoni, documenti o contrassegni di copertura); - richiedere informazioni a istituti finanziari, aziende postali, compagnie aeree e aziende di telecomunicazione; - accedere a diverse banche dati gestite dalla Repubblica federale (per es. al registro centrale degli stranieri del <i>Bundesamt für Migration und Flüchtlinge</i>, ai dati in materia di asilo del <i>Bundesamt für die Anerkennung ausländischer Flüchtlinge</i> oppure al registro dei veicoli). Per quanto riguarda l'osservazione di organizzazioni e individui sono necessari indizi concreti per sospettare attività che minacciano la Costituzione o la sicurezza. <i>BND:</i> i mezzi di intelligence utilizzati all'estero o concernenti l'estero (soprattutto HUMINT e l'esplorazione delle telecomunicazioni) non sono disciplinati nella legislazione, mentre lo sono le attività del BND sul territorio tedesco. In sintonia con la legge tedesca sulla protezione dei dati può rilevare, elaborare e utilizzare le informazioni necessarie, compresi i dati riferiti a persone: - per proteggere i propri collaboratori, le proprie installazioni, i propri beni e le proprie fonti contro attività che minacciano la sicurezza o contro lo spionaggio; - per il controllo di sicurezza relativo a persone che sono o saranno attive in seno al BND; - per la verifica degli accessi alle informazioni necessari all'adempimento dei compiti; - per l'acquisizione di informazioni su fatti all'estero rilevanti in materia di politica estera e di politica di sicurezza per la Repubblica federale di Germania, se sono ottenibili unicamente in questo modo e nessun'altra autorità è competente per il loro rilevamento. Se è necessario per adempiere i compiti, il BND può nel singolo caso richiedere informazioni su dati a operatori postali e di teleservizi, compagnie aeree e istituti di credito. Inoltre, può impiegare metodi, oggetti e mezzi per acquisire segretamente informazioni (per es. impiego di persone di fiducia o informatori, osservazioni, registrazioni di immagini e suoni, documenti o contrassegni di copertura). Per quanto riguarda la sorveglianza della corrispondenza postale e delle telecomunicazioni, il BfV e il BND sottostanno alla <i>Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses</i>. Pertanto, misure incisive in questo ambito possono necessitare dell'autorizzazione dell'organo di controllo parlamentare oppure della commissione G-10.

	Entrambi i servizi non hanno né poteri di polizia né facoltà di emanare istruzioni.
Vigilanza	<i>BfV/BND:</i> - l'organo di controllo parlamentare ha diritto, per il controllo attivo, di consultare atti e dati dei servizi informazioni, interrogare collaboratori, effettuare visite e, in singoli casi, di ricorrere all'assistenza di esperti. Inoltre, il Governo federale è tenuto a informare l'organo in merito alle attività dei servizi informazioni, tranne che se vi sono i presupposti per rifiutare l'informazione, ad esempio per motivi imperativi di protezione delle fonti. L'organo partecipa anche alla procedura decisionale relativa alle misure nell'ambito della cosiddetta sorveglianza strategica. - Le Commissioni parlamentari d'inchiesta possono essere istituite, su richiesta di un quarto dei deputati del Bundestag, per chiarire fatti gravi nel campo dell'intelligence. Questo strumento non esercita una funzione di controllo costante. Vi è però un ampio obbligo di presentare gli atti per tutti gli organi pubblici nonché un obbligo di testimoniare per i rappresentanti governativi e i collaboratori dei servizi informazioni. - I servizi informazioni sono controllati anche nel quadro dell'«Artikel-10-Gesetz». L'organo parlamentare e la Commissione G-10 si completano nel controllo della sorveglianza della corrispondenza postale e delle telecomunicazioni. Inoltre, la Commissione G-10 decide in merito all'ammissibilità e alla necessità di misure di limitazione nell'ambito del controllo individuale e strategico. Di conseguenza, informa il ministero responsabile del rispettivo servizio informazioni in merito alle misure previste per la sorveglianza strategica delle telecomunicazioni. La Commissione può anche verificare l'intero rilevamento, trattamento e utilizzo dei dati riferiti a persone acquisiti grazie alla sorveglianza della corrispondenza postale e delle telecomunicazioni, non da ultimo grazie al diritto all'informazione, alla consultazione di documenti e all'accesso a tutti i locali di servizio. - Il Comitato parlamentare di fiducia è competente per il controllo del bilancio dei servizi informazioni. - La Corte federale dei conti verifica i conti annuali nonché la gestione del bilancio e la gestione economica. - L'incaricato federale per la protezione dei dati e la libertà d'informazione verifica sia per quanto riguarda il servizio informazioni interno sia per il servizio informazioni concernente l'estero l'osservanza della legge tedesca sulla protezione dei dati e delle altre prescrizioni per la protezione dei dati.
Protezione dei dati	<i>BfV/BND:</i> la gestione dei dati riferiti a persone da parte dei servizi e i diritti delle persone interessate sono disciplinati nella legislazione in materia di servizi informazioni. Le regolamentazioni per il <i>BfV</i> e il <i>BND</i> sono praticamente identiche. Il <i>BfV</i> può memorizzare, modificare e utilizzare dati riferiti a persone se vi sono indizi concreti per sospettare attività che minacciano la Costituzione o la sicurezza, il <i>BND</i> può fare altrettanto sempre che l'adempimento dei propri compiti lo richieda. In caso di inesattezze, i dati devono tuttavia essere corretti e in caso di illiceità, oppure se non sono più necessari, cancellati. Ciò viene verificato in singoli casi oppure entro i termini stabiliti (<i>BfV</i>: dopo cinque anni; <i>BND</i>: dopo dieci anni). I dati riferiti a persone che pregiudicano interessi degni di protezione delle persone in questione e non sono più necessari per il futuro adempimento dei compiti devono essere bloccati. Se una persona può richiamare l'attenzione su una fattispecie concreta e far valere un particolare interesse a un'informazione, riceve gratuitamente informazioni in merito ai dati concernenti la propria persona. A determinate condizioni i dati riferiti a persone possono essere comunicati ad autorità estere, a servizi delle forze armate di stazionamento nonché a organi sovranazionali e internazionali. A determinate condizioni il <i>BND</i> può ottenere dati riferiti a persone da altre autorità tedesche.

	Francia <i>Direction centrale du renseignement intérieur (DCRI)</i> <i>Direction générale de la sécurité extérieure (DGSE)</i> Il libro bianco francese del 2008 prevede l'elaborazione di un quadro legale per le attività dei servizi informazioni francesi, tuttavia le loro attività sinora non sono praticamente state disciplinate.
Posizione nell'architettura di sicurezza	<i>DCRI:</i> il servizio informazioni interno è subordinato al Ministero dell'interno. <i>DGSE:</i> il servizio informazioni concernente l'estero è subordinato al Ministero della difesa. In Francia la comunità dell'intelligence comprende diversi servizi complementari. Oltre alla <i>DCRI</i> e alla <i>DGSE</i> vi sono altri sei servizi.
Compiti	<i>DCRI:</i>

	- prevenire e reprimere attività ispirate, svolte o sostenute da potenze e organizzazioni estere e tali da minacciare la sicurezza del Paese; - contribuire a prevenire e reprimere atti di terrorismo o azioni che minacciano l'autorità dello Stato, il segreto di Stato oppure il patrimonio economico del Paese; - contribuire alla sorveglianza delle radiocomunicazioni e delle comunicazioni elettroniche che minacciano la sicurezza dello Stato nonché contribuire alla lotta contro la criminalità nel settore delle tecnologie dell'informazione e della comunicazione; - partecipare alla sorveglianza di persone, gruppi, organizzazioni e fenomeni sociali che con il loro carattere radicale, il loro orientamento o i loro effetti minacciano la sicurezza nazionale. <i>DGSE:</i> - acquisire e valutare informazioni rilevanti per la sicurezza della Francia a favore del Governo e in collaborazione con altre organizzazioni; - individuare o ostacolare le attività di spionaggio che al di fuori del territorio francese sono dirette contro interessi francesi (nel senso di una misura preventiva); - al riguardo, la <i>DGSE</i> assicura i collegamenti necessari con altri servizi e organizzazioni rilevanti, esegue le operazioni che le sono assegnate dal Governo nell'ambito della propria competenza e presenta le informazioni raccolte sottoforma di sintesi; - in tale contesto, la <i>DGSE</i> considera in particolare la lotta al terrorismo e la lotta contro la proliferazione delle armi di distruzione di massa, ma anche il servizio informazioni militare e il servizio informazioni strategico.
Competenze (impiego di mezzi di intelligence)	<i>DCRI:</i> la DCRI collabora con gli Esecutivi delle regioni e le prefetture della Polizia nazionale. Le sue competenze non sono ancora disciplinate nella legislazione. <i>DGSE:</i> la DGSE acquisisce informazioni tramite tutti i metodi informativi: HUMINT, SIGINT, OSINT e mezzi operativi. Collabora con servizi informazioni francesi ed esteri. Effettua operazioni segrete tramite agenti paramilitari. Metodi e competenze non sono disciplinati nella legislazione.
Vigilanza	<i>DCRI/DGSE:</i> - la Délégation parlementaire au renseignement (Delegazione parlamentare per i servizi informazioni) vigila sulle attività e sui mezzi. La Delegazione riceve informazioni sul budget, sulle attività generali e sull'organizzazione dei servizi informazioni, tuttavia non riceve informazioni sulle attività operative, sulle disposizioni governative, sul relativo finanziamento e sugli scambi con servizi esteri o organizzazioni internazionali. Non rientrano tra le informazioni accessibili quelle che potrebbero compromettere l'anonimato, la sicurezza o la vita di una persona o quelle che rivelerebbero specifici metodi operativi per raccogliere informazioni. Il lavoro della delegazione parlamentare sottostà al segreto di Stato. Formula raccomandazioni e osservazioni e redige un rapporto annuale. - Altre autorità di controllo: – la Commission nationale de contrôle des interceptions de sécurité per la sorveglianza di intercettazioni ambientali; – la Commission nationale de l'informatique et des libertés per il controllo della protezione dei dati; – la Commission de vérification des fonds spéciaux per l'assegnazione di risorse finanziarie speciali ai servizi informazioni.
Protezione dei dati	<i>DCRI/DGSE:</i> per i servizi informazioni non sono state definite condizioni specifiche in materia di protezione dei dati. I servizi informazioni sottostanno tuttavia alle disposizioni generali in materia di protezione dei dati e al controllo della <i>Commission nationale de l'informatique et des libertés</i>. Quest'ultima controlla l'osservanza della legge sulla protezione dei dati e la gestione dei dati riferiti a persone da parte dei servizi informazioni e, su incarico dei cittadini interessati, esercita il loro diritto di visionare gli atti, che nel contesto dei servizi informazioni francesi può essere concretizzato soltanto in questa maniera indiretta.

	Spagna <i>Centro Nacional de Inteligencia (CNI)</i>
Posizione nell'architettura di sicurezza	Il CNI è subordinato al Ministero della difesa. Dirige la comunità dell'intelligence spagnola. È completato da un servizio informazioni militare e da altri servizi informazioni minori.
Compiti	- Raccogliere, valutare ed elaborare informazioni in Spagna e all'estero per proteggere e promuovere gli interessi politici, economici e industriali, commerciali e strategici del Paese. - Prevenire, scoprire e neutralizzare attività di servizi esteri, gruppi o persone che minacciano, violano o costituiscono un rischio per l'ordinamento costituzionale, i diritti o le libertà dei cittadini spagnoli, la

	sovranità, e l'integrità o la sicurezza dello Stato, la stabilità delle istituzioni, gli interessi economici nazionali o il benessere della popolazione. - Promuovere i rapporti e la collaborazione con i servizi informazioni di altri Paesi e con le organizzazioni internazionali. - Eseguire l'acquisizione, la valutazione e l'interpretazione in ambito SIGINT. - Coordinare i diversi servizi, utilizzare i metodi di crittaggio e garantire la sicurezza delle tecnologie dell'informazione in questo settore. Inoltre, acquistare materiale per la crittologia e provvedere alla formazione del personale. - Controllare l'osservanza delle regolamentazioni per la protezione di informazioni segrete. - Garantire la sicurezza e la protezione delle proprie installazioni, informazioni e risorse materiali e di personale.
Competenze (impiego di mezzi di intelligence)	Le competenze del <i>CNI</i> sono soltanto in parte disciplinate nella legislazione, l'impiego dei mezzi di intelligence sottostà al controllo giudiziario. Il <i>CNI</i> adempie i suoi compiti raccogliendo informazioni mediante mezzi di intelligence sia in Spagna che all'estero. Può svolgere indagini di sicurezza su persone ed entità e al riguardo può contare sulla necessaria collaborazione di organizzazioni e istituzioni pubbliche e private. L'uso dei mezzi di intelligence non è disciplinato in maniera univoca, tuttavia un disciplinamento risulta dall'autorizzazione che può essere ottenuta per l'impiego di mezzi che incidono sull'inviolabilità della sfera privata o la confidenzialità del traffico di dati (per es. sorveglianza e intercettazione). Il <i>CNI</i> può ottenere questa autorizzazione mediante richiesta del direttore al giudice competente della Corte suprema, sempre che l'impiego dei mezzi sia necessario per l'adempimento dei compiti. La richiesta deve avvenire in maniera formale e scritta e specificare le misure necessarie, le circostanze, gli obiettivi e i motivi di tali misure. Inoltre, deve contenere indicazioni concernenti le persone interessate e il luogo in cui saranno impiegate le misure. Il giudice competente è tenuto a decidere entro 72 ore (in casi urgenti entro 24 ore). Il <i>CNI</i> dispone di mezzi per inchieste mascherate e può ricevere dalle autorità competenti le identità, le immatricolazioni e i documenti necessari alle sue missioni. Agli agenti del <i>CNI</i> è consentito il porto d'armi in conformità con le relative esigenze e le prescrizioni legali. A prescindere dal personale addetto alla sicurezza, il servizio informazioni spagnolo non dispone tuttavia di alcun potere di polizia.
Vigilanza	Il comitato parlamentare per la vigilanza sui fondi segreti è competente per il controllo parlamentare. Verifica gli obiettivi assegnati dal Governo e il rapporto annuale del direttore del <i>CNI</i> sulle attività e sulla situazione per quanto riguarda gli obiettivi assegnati. Il comitato ha accesso unicamente alle informazioni che non si riferiscono a fonti o risorse del <i>CNI</i> oppure che non provengono da servizi informazioni esteri o da organizzazioni internazionali. Inoltre, il comitato non può appropriarsi di alcun documento, nemmeno di copie. L'impiego dei mezzi di intelligence sottostà al controllo giudiziario.
Protezione dei dati	I testi di legge che concernono il <i>CNI</i> non menzionano questioni relative alla protezione dei dati né rimandano a una legge nazionale sulla protezione dei dati a cui si dovrebbe attenere il servizio informazioni spagnolo.

	Paesi Bassi <i>Algemene Inlichtingen- en Veiligheidsdienst (AIVD)</i>
Posizione nell'architettura di sicurezza	L'<i>AIVD</i> è subordinato al Ministero dell'interno. È completato dal servizio informazioni militare.
Compiti	- Indagini su persone e organizzazioni per le quali sussiste un sospetto fondato che rappresentino un serio pericolo per l'ordinamento democratico, la sicurezza nazionale o altri importanti interessi dei Paesi Bassi. - Esame dei candidati a posizioni con obbligo del segreto. - Appoggio alle istituzioni responsabili della sicurezza dell'infrastruttura nazionale privata e pubblica di importanza vitale per il mantenimento della struttura sociale olandese. - Indagini su Paesi in conformità con attività affidate per incarico congiunto del Primo ministro, del ministro dell'interno e del ministro della difesa. - Elaborazione di analisi dei rischi e dei pericoli relative a immobili, prestazioni e individui per il sistema nazionale di sicurezza
Competenze (impiego di)	Le competenze dell'<i>AIVD</i> sono disciplinate in maniera relativamente chiara nella legislazione, l'impiego dei mezzi di intelligence da parte dell'<i>AIVD</i> è regolamentato da una moltitudine di condizioni nella legge

mezzi di intelligence)	sui servizi informazioni e sul servizio di sicurezza. Per l'acquisizione di informazioni dispone delle competenze seguenti: - contattare tutte le autorità o persone che sembrano in grado di fornire le informazioni necessarie; - sorvegliare persone e opere con o senza ausili tecnici per effettuare registrazioni, inseguire tracce o procedere alla localizzazione; - impiegare agenti infiltrati; - perquisire opere e settori chiusi; - aprire lettere e invii di merci senza il consenso del mittente o del destinatario (è però necessario il mandato del tribunale distrettuale dell'Aia); - accedere a sistemi di ordinatori con o senza mezzi tecnici o segni, password e identità falsi; - intercettare, registrare o sorvegliare qualsiasi forma di conversazione, telecomunicazioni o trasferimento di dati con l'ausilio di apparecchi tecnici; - rivolgersi a operatori pubblici di reti di telecomunicazioni per informazioni su un utente. Queste competenze sottostanno a rigorose condizioni legali e necessitano spesso di un'istruzione del ministro competente o del direttore del servizio informazioni. L'AIVD non ha alcun potere di polizia e non gli è consentito di occuparsi di reati.
Vigilanza	- Un comitato parlamentare di vigilanza sui servizi informazioni e sui servizi di sicurezza controlla l'osservanza della legge sui servizi informazioni e di sicurezza da parte del servizio informazioni civile e militare. Tutti i partecipanti al processo di intelligence sono tenuti a collaborare con il comitato. Inoltre, il comitato ha accesso a tutte le informazioni di intelligence e ha il diritto di interrogare testimoni ed esperti e di avviare un'inchiesta. - L'ombudsman nazionale è competente per i ricorsi della popolazione concernenti il comportamento dei servizi informazioni e dei servizi di sicurezza. Decide in merito a tali ricorsi e motiva la sua posizione, sempre che la sicurezza e altri interessi dello Stato non vi si oppongano. Successivamente informa il ministro interessato in merito alla sua decisione. L'ombudsman può anche formulare raccomandazioni. Il ministro trasmette poi le raccomandazioni e le sue conclusioni al Parlamento olandese. - La Corte dei conti verifica le uscite dell'AIVD per le operazioni segrete e presenta annualmente al Parlamento un rapporto al riguardo. - I ministri responsabili dei servizi informazioni e dei servizi di sicurezza presentano al Parlamento un rapporto annuale sulle attività dell'AIVD.
Protezione dei dati	L'AIVD può utilizzare o elaborare i dati personali di una persona unicamente nei casi seguenti: - se sussiste un serio sospetto che questa persona costituisca un pericolo per l'ordinamento democratico, la sicurezza o altri interessi vitali del Paese; - se la persona ha dato il proprio consenso per effettuare un controllo di sicurezza; - se ciò è necessario nell'ambito di ricerche su altri Paesi; - se le informazioni sono state raccolte da un altro servizio informazioni o da un altro servizio di sicurezza; - se i dati sono necessari al servizio affinché questo possa adempiere i propri obblighi; - se la persona è stata o è impiegata presso il servizio; oppure - se i dati sono necessari all'allestimento di analisi dei rischi. Se i dati riferiti a persone non hanno più alcuna importanza per lo scopo per il quale sono stati raccolti, devono essere eliminati. Anche le informazioni che si sono rivelate errate o che sono state elaborate illecitamente devono essere corrette o eliminate. Il ministro, altre persone e autorità rilevanti, i servizi informazioni e i servizi di sicurezza rilevanti di altri Paesi nonché le organizzazioni di sicurezza, le organizzazioni SIGINT e le organizzazioni di intelligence internazionali rilevanti possono essere informati in merito alle informazioni elaborate dall'AIVD. Per quanto riguarda il diritto di consultare dati personali, il ministro competente è tenuto a informare appena possibile il richiedente in merito a quali dati personali sono stati elaborati dal servizio o per il servizio. Successivamente il richiedente ha il diritto di consultare i dati.

	Austria <i>Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (BVT)</i> <i>Heeresnachrichtenamt (HNA)</i>
Posizione nell'architettura di sicurezza	BVT: il servizio informazioni interno è subordinato, in quanto parte della polizia di sicurezza, alla Direzione generale della sicurezza pubblica in seno al Ministero federale dell'interno. Il BVT è appoggiato da nove uffici dei Länder per la tutela della Costituzione e la lotta al terrorismo. HNA:

	il servizio informazioni strategico concernente l'estero è subordinato, in seno al Ministero federale della difesa e dello sport, al capo di Stato maggiore generale. Oltre al servizio informazioni interno e al servizio informazioni concernente l'estero vi è un unico servizio supplementare, il Servizio per le informazioni e la sicurezza militare, che svolge la funzione di servizio informazioni militare.
Compiti	<i>BVT:</i> - acquisizione di informazioni, indagini e analisi nei settori del terrorismo, dell'estremismo, del controspionaggio, del traffico illegale di armi e della proliferazione; - protezione di persone e di opere per gli esponenti di istituzioni costituzionali; - protezione di rappresentanti di Stati esteri, organizzazioni internazionali e altri oggetti tutelati dal diritto internazionale pubblico; - protezione di infrastrutture critiche; - controlli di sicurezza. <i>HNaA:</i> attività informativa: acquisizione, elaborazione, valutazione e presentazione di informazioni concernenti l'estero o organizzazioni internazionali oppure altri enti internazionali in relazione con fattispecie militari e altri fatti, fenomeni o progetti connessi.
Competenze (impiego di mezzi di intelligence)	L'impiego di mezzi di intelligence è disciplinato chiaramente dalla legge per entrambi i servizi. <i>BVT:</i> il <i>BVT</i> acquisisce le sue informazioni tramite la valutazione di OSINT nonché da fonti non aperte. In questo ambito (ricerca ampliata in materia di pericoli) dispone delle seguenti competenze: - sorveglianza di gruppi di persone, se sulla base delle circostanze e degli sviluppi è possibile prevedere un serio pericolo per la sicurezza pubblica e a causa della criminalità ad esso correlata, segnatamente la violenza a sfondo religioso o ideologico; - impiego segreto di apparecchi per riconoscere le targhe dei veicoli e impiego visibile di apparecchi per registrare immagini e suoni nelle aree critiche in materia di criminalità; - impiego segreto di apparecchi per registrare immagini e suoni e la trasmissione di registrazioni private di suoni e immagini alle autorità di sicurezza a determinate condizioni; - osservazioni e impiego di agenti infiltrati. A seconda dell'entità dell'impatto dei mezzi di intelligence, il loro utilizzo presuppone l'informazione del garante dei rimedi giuridici del Ministero federale dell'interno e l'autorizzazione preliminare del suddetto garante. Il <i>BVT</i> è un servizio di polizia e quindi, in quanto parte della polizia di sicurezza, ha poteri di polizia conformemente alla <i>Sicherheitspolizeigesetz</i>. <i>HNaA:</i> secondo la <i>Militärbefugnisgesetz</i> l'<i>HNaA</i> ha le seguenti competenze in materia di intelligence: - richiesta di informazioni a persone, organi di enti territoriali e di altri enti di diritto pubblico nonché a fondazioni, istituti e fondi gestiti da questi enti e agli operatori di servizi di telecomunicazione pubblici; - rilevamento di dati mediante osservazione, se altrimenti l'adempimento dei compiti sarebbe impedito o ostacolato in maniera considerevole; - inchiesta mascherata, se ciò è urgentemente necessario nell'interesse della sicurezza nazionale, segnatamente nell'interesse della garanzia della prontezza all'impiego dell'esercito austriaco e se altrimenti sarebbe impedito l'adempimento dei compiti; - rilevamento di dati mediante apparecchi per registrare immagini e suoni, se ciò è indispensabile nell'interesse della sicurezza nazionale, segnatamente nell'interesse della garanzia della prontezza all'impiego dell'esercito austriaco, e se altrimenti l'adempimento dei compiti sarebbe in gran parte impedito. Prima di un rilevamento dei dati mediante osservazione, inchiesta mascherata o apparecchi per registrare immagini e suoni, l'<i>HNaA</i> deve informare il garante dei rimedi giuridici per la verifica della legalità delle misure in materia di intelligence o di controspionaggio, indicando i motivi principali del rilevamento, nonché comunicarlo al ministro federale della difesa. Un simile rilevamento può essere avviato unicamente dopo il pertinente consenso del garante dei rimedi giuridici. Se un'ulteriore attesa dovesse però comportare un grave danno per la sicurezza nazionale a cui non è più possibile rimediare, segnatamente per la prontezza all'impiego dell'esercito austriaco o per la sicurezza delle persone, il rilevamento potrà essere avviato ed effettuato immediatamente dopo la presa di conoscenza da parte del garante dei rimedi giuridici, sempre che quest'ultimo non vi ponga fine con un veto.
Vigilanza	<i>BVT:</i> - controlli nel quadro dell'<i>Interpellationsrecht</i>, il diritto del Parlamento di controllare la gestione dell'Esecutivo.

	- Controlli da parte dello Ständiger Unterausschuss des Ausschusses für innere Angelegenheiten zur Überprüfung von Massnahmen zum Schutz der verfassungsmässigen Einrichtungen und ihrer Handlungsfähigkeit (sottocomitato permanente della Commissione per gli affari interni incaricata della verifica delle misure volte alla protezione delle istituzioni costituzionali e della loro capacità di agire). Esso è competente per la verifica dell'adempimento dei compiti conforme alla Costituzione da parte del BVT. È autorizzato dal ministro federale dell'interno a richiedere informazioni e a consultare documenti. - Controllo sostanzialmente amministrativo da parte della Corte dei conti e della Difesa civica (Volksanwaltschaft). - Controlli da parte del garante dei rimedi giuridici del Ministero federale dell'interno. Nel quadro delle competenze speciali del BVT il suo coinvolgimento spazia, a seconda dell'intensità dell'impatto delle misure, dalla semplice presa di conoscenza all'autorizzazione preliminare per le misure. Allestisce annualmente un rapporto sull'adempimento dei propri compiti. - Controlli da parte del Comitato per i diritti dell'uomo (Menschenrechtsbeirat). Esso consiglia il ministro federale dell'interno in caso di questioni concernenti la tutela dei diritti dell'uomo e in questa funzione vigila anche sul BVT. Questo è tenuto ad assisterlo nella sua attività, inoltre il ministro federale gli mette a disposizione le risorse necessarie all'adempimento dei compiti. <i>HNaA:</i> - controlli nel quadro dell'<i>Interpellationsrecht</i>, il diritto del Parlamento di controllare la gestione dell'Esecutivo. - Controlli da parte dello Ständiger Unterausschuss des Landesverteidigungsausschusses zur Überprüfung von nachrichtendienstlichen Massnahmen zur Sicherung der militärischen Landesverteidigung (sottocomitato permanente della Commissione per la difesa nazionale incaricato della verifica delle misure di intelligence volte alla sicurezza della difesa nazionale militare). Esso può esigere dall'<i>HNaA</i> tutte le informazioni e i documenti pertinenti. Ai fini della protezione delle fonti non è tuttavia autorizzato a richiedere informazioni o documenti, in particolare sulle fonti, la cui conoscenza potrebbe minacciare la sicurezza nazionale o la sicurezza delle persone. - Controlli da parte del garante dei rimedi giuridici per verificare la legalità delle misure in materia di intelligence o di controspionaggio. Esso è competente per l'autorizzazione e il controllo dell'impiego dei mezzi di intelligence. Gli si deve accordare in ogni momento il diritto di consultare tutti i documenti e le registrazioni necessari nonché fornirgli le informazioni necessarie. Ciò non vale tuttavia per le informazioni e i documenti, relativi all'identità di persone o a fonti, la cui conoscenza potrebbe minacciare la sicurezza nazionale o la sicurezza delle persone. Deve pure poter sorvegliare in ogni momento l'attuazione delle misure che deve controllare e accedere a tutti i locali in cui sono conservati registrazioni o altri risultati della sorveglianza. Inoltre, il garante dei rimedi giuridici vigila sull'osservanza dell'obbligo di rettifica o cancellazione conformemente alle disposizioni in materia di protezione dei dati. Allestisce un rapporto annuale sulle proprie attività. <i>BVT/HNaA:</i> controlli da parte della Commissione per la protezione dei dati. Nel quadro della legge sulla protezione dei dati la Commissione è competente per la protezione giuridica di una persona fisica in caso di sospette violazioni del diritto fondamentale alla protezione dei dati. Essa giudica i ricorsi per sospetta violazione del diritto all'informazione, alla tutela del segreto, alla rettifica o alla cancellazione.
Protezione dei dati	<i>BVT:</i> La gestione dei dati riferiti a persone e i diritti delle persone interessate sono disciplinati dalla <i>Sicherheitspolizeigesetz</i>. I dati riferiti a persone possono essere rilevati e utilizzati, sempre che ciò sia necessario per l'adempimento dei compiti. I dati possono essere richiesti anche agli operatori di servizi di telecomunicazione o ad altri fornitori di servizi. I dati inesatti o rilevati in maniera imprecisa devono essere rettificati e i dati riferiti a persone non più necessari devono essere cancellati. I dati elaborati riferiti a persone devono essere verificati se non sono più stati modificati per sei anni. Un interessato ha il diritto di ricevere gratuitamente informazioni in merito ai dati rilevati concernenti la propria persona. Il BVT non deve tuttavia fornire alcuna informazione se ciò è necessario alla protezione del fornitore delle informazioni o se legittimi interessi preponderanti del mandante o di un terzo, segnatamente interessi pubblici preponderanti (per es. la protezione delle istituzioni costituzionali della Repubblica d'Austria) ai oppongono alla comunicazione delle informazioni. <i>HNaA:</i> la <i>Militärbefugnisgesetz</i> non prevede regolamentazioni speciali relative alla protezione dei dati, ma rimanda alla legge sulla protezione dei dati. Un interessato ha il diritto di ricevere gratuitamente informazioni in merito ai dati rilevati concernenti la propria persona. Il BVT non deve tuttavia fornire alcuna informazione se ciò è necessario alla protezione del fornitore delle informazioni o se legittimi interessi preponderanti del mandante o di un terzo, segnatamente interessi pubblici preponderanti (per es. la garanzia della prontezza all'impiego dell'esercito

	austriaco o gli interessi della difesa nazionale), si oppongono alla comunicazione delle informazioni.
--	--

	Belgio <i>Sûreté de l'Etat (SE)</i> <i>Service générale du renseignement et de la sécurité des Forces armées (SGRS)</i> (In Belgio la SE è di carattere civile, il SGRS di orientamento militare. Entrambi sono competenti per l'intelligence sia interna sia esterna, tuttavia la SE si occupa essenzialmente dell'interno mentre il SGRS si concentra piuttosto sull'estero).
Posizione nell'architettura di sicurezza	SE: il servizio informazioni civile è in generale subordinato al Ministro della giustizia, per le questioni che riguardano la sicurezza pubblica e la protezione delle persone è tuttavia competente anche il Ministro dell'interno. SGRS: Il servizio informazioni militare è subordinato al Ministro della difesa. Anche il servizio delle dogane e la polizia si occupano dell'acquisizione informativa, ma non sono servizi informazioni veri e propri e quindi non sottostanno alle relative leggi. I servizi informazioni collaborano sia tra di loro sia con servizi esteri e possono fornire appoggio alle autorità giudiziarie e amministrative.
Compiti	SE: - ricercare, analizzare e elaborare informazioni su attività che minacciano o potrebbero minacciare la sicurezza dello Stato o l'esistenza dell'ordinamento democratico o costituzionale, la sicurezza esterna dello Stato o le relazioni internazionali, il potenziale scientifico o economico o tutti gli altri interessi fondamentali del Paese (spionaggio, terrorismo, estremismo, proliferazione delle armi di distruzione di massa, organizzazioni settarie nocive o organizzazioni criminali, interferenze). - controlli di sicurezza; - protezione delle persone; - altri compiti secondo la legge. SGRS: - ricercare, analizzare e elaborare informazioni su attività che minacciano o potrebbero minacciare l'integrità del territorio nazionale, i piani di difesa militari, l'esecuzione dei compiti delle Forze armate, la sicurezza dei cittadini belgi o altri interessi fondamentali del Paese; informare il ministro competente; - consigliare il Governo nelle questioni di politica estera e di difesa; - tutelare la sicurezza militare del personale del Ministero della difesa, delle installazioni militari, delle armi, dei piani, dei sistemi informatici, delle comunicazioni e di altre opere militari; - tutela del segreto; - controlli di sicurezza.
Competenze (impiego di mezzi di intelligence)	L'impiego dei mezzi di intelligence è disciplinato in maniera chiara per entrambi i servizi nella legislazione. SE/SGRS: Conformemente alla legge, i servizi possono ricercare, raccogliere, ricevere e elaborare dati riferiti a persone, sempre che ciò sia necessario per adempiere i propri compiti. Inoltre, per ottenere informazioni possono ricorrere a autorità giudiziarie, funzionari e impiegati del servizio pubblico nonché a persone o organizzazioni del settore privato, entrare in locali e luoghi pubblicamente accessibili, visitare alberghi e altri alloggi nonché utilizzare fonti umane. Se questi metodi usuali non sono sufficienti per ottenere informazioni, entrambi i servizi possono utilizzare anche metodi specifici o metodi straordinari. Metodi specifici: - osservazione mediante ausili tecnici in spazi pubblici o privati accessibili al pubblico oppure osservazione con o senza ausili tecnici di spazi privati non accessibili al pubblico; - controlli di spazi pubblici e di spazi privati accessibili al pubblico nonché di opere chiuse che si trovano al loro interno mediante ausili tecnici; - identificazione del mittente o del destinatario di un invio postale o del titolare di una casella postale; - identificazione dell'abbonato o dell'utente abituale di un servizio di comunicazione elettronica o del mezzo di comunicazione elettronica utilizzato; - localizzazione dei dati relativi alle chiamate di mezzi di comunicazione elettronica e localizzazione della provenienza o della destinazione della comunicazione elettronica.

	Questi metodi possono essere utilizzati soltanto se la commissione amministrativa istituita per la sorveglianza e in parte anche per l'autorizzazione dei metodi è stata informata al riguardo dal direttore del rispettivo servizio. Metodi straordinari: - osservazione e controllo di spazi privati non accessibili al pubblico; - costituzione e utilizzazione di una persona giuridica per appoggiare le attività operative e l'impiego di agenti; - apertura e lettura della posta; - raccolta di dati relativi a conti bancari e transazioni bancarie; - intrusione in un sistema informatico; - intercettazione e registrazione di comunicazioni. Questi metodi possono essere utilizzati soltanto se sono stati autorizzati dalla commissione amministrativa competente. I servizi informazioni belgi possono appoggiare le autorità giudiziarie, ma non hanno però poteri di polizia (per lo meno la legge non si esprime al riguardo).
Vigilanza	<i>SE/SGRS:</i> - commissione permanente per i servizi informazioni e i servizi di sicurezza (autorità di controllo parlamentare): vigila sui servizi informazioni e può svolgere indagini (inoltre dispone del diritto di visionare gli atti e può disporre convocazioni, perquisizioni e sequestri). - Commissione amministrativa: sorveglia l'applicazione delle misure specifiche e delle misure straordinarie dei servizi informazioni. - Ombudsman federale: è competente per i ricorsi di singoli individui, può svolgere indagini e visionare atti; non sussiste però alcun obbligo di trasmettergli informazioni segrete. - Commissione per la protezione dei dati: verifica su incarico dei cittadini le informazioni riferite a persone rilevate dai servizi, può però formulare unicamente raccomandazioni e non può fornire informazioni in merito al contenuto degli atti.
Protezione dei dati	<i>SE/SGRS:</i> Alla <i>SE</i> e al <i>SGRS</i> si applicano le stesse regolamentazioni. La gestione da parte dei servizi dei dati riferiti a persone e i diritti delle persone interessate sono disciplinati nella legislazione in materia di attività informative. Le informazioni e i dati riferiti a persone possono essere ricercati, raccolti, ricevuti ed elaborati. Possono anche essere comunicati a determinate persone, autorità, servizi di polizia o a tutti gli altri organi competenti, sempre che questi siano oggetto di una minaccia oppure le informazioni riferite a persone siano utili all'adempimento dei propri compiti. Questi dati possono essere conservati soltanto finché sono necessari per lo scopo per cui sono stati registrati, ad eccezione dei dati considerati di importanza storica dall'Archivio di Stato. La distruzione avviene soltanto dopo la scadenza di un termine stabilito dal re e basato sull'ultima elaborazione dei dati. I cittadini non hanno alcun diritto di visionare gli atti personali che li concernono e devono rivolgersi alla commissione per la protezione dei dati.