CAMERA DEI DEPUTATI

XVI LEGISLATURA

SERVIZIO BIBLIOTECA

MATERIALI DI LEGISLAZIONE COMPARATA

LA DISCIPLINA DELLE INTERCETTAZIONI

N. 2 – Giugno 2008

UFFICIO LEGISLAZIONE STRANIERA

Indice

DOCUMENTAZIONE

FRANCIA

Code de procedure penale (Partie Législative)

Loi n° 91-646 du 10 juillet 1991. Loi relative au secret des correspondances émises par la voie des communications électroniques.

GERMANIA

Legge fondamentale

Strafprozessordnung

Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz - G 10)

Gesetz über das Zollkriminalamt und die Zollfahndungsämter (Zollfahndungsdienstgesetz - ZFdG)

REGNO UNITO

Regulation of Investigatory Powers Act 2000. Part I Communications. Chapter IInterception

SPAGNA

Costituzione

Ley de enjuiciamiento criminal

Premessa

La presente pubblicazione aggiorna il dossier “La disciplina delle intercettazioni”, della collana “Materiali di legislazione comparata”, n. 2 della XV Legislatura, uscito nel settembre 2006.

Le novità di maggiore rilievo riguardano, in particolare, la Germania, dove nel 2007 sono state approvate, nell’ordine, la modifica della normativa sui servizi investigativi doganali e di altre leggi, del 12 giugno 2007, e la legge di riforma della disciplina sulle intercettazioni telefoniche e su altre misure investigative nascoste, del 21 dicembre 2007.

Schede di sintesi

FRANCIA

Il quadro normativo

Il segreto della corrispondenza emessa attraverso le telecomunicazioni è garantito dalla legge, le intercettazioni sono dunque delle misure a carattere eccezionale che derogano al principio della segretezza, in un quadro giuridico definito dalla legge n. 91-646 del 10 luglio 1991, che ne consente il ricorso solo da parte della pubblica autorità e per tutelare un interesse pubblico. La legge distingue due tipi di intercettazioni: giudiziarie e amministrative o di sicurezza.

Per telecomunicazioni, ai sensi dell'articolo 32 del Codice delle poste e delle comunicazioni elettroniche, si intendono "tutte le trasmissioni, emissioni o ricezioni di segni, segnali, scritti, immagini, suoni o informazioni di qualsiasi natura emessi attraverso filo, fibre ottiche, radioelettricità o altri sistemi elettromagnetici".

Le intercettazioni giudiziarie

L'intercettazione di conversazioni telefoniche, in ambito giudiziario, anche se abitualmente praticata, non ha avuto in Francia alcuna regolamentazione specifica, trovando fondamento legale unicamente nella previsione generale dell'articolo 81 c.p.p. relativo ai poteri del giudice istruttore. Tale situazione ha dato luogo ad abusi che hanno portato alla condanna della Francia da parte della Corte europea dei diritti dell'uomo. In seguito alla pronuncia della Corte, il legislatore ha disciplinato la materia con la già citata legge del 10 luglio 1991, che ha modificato il codice di procedura penale, inserendovi gli articoli da 100 a 100-7.

L'articolo 100 definisce il quadro giuridico in base al quale possono essere disposte le intercettazioni di corrispondenza effettuate tramite le vie di telecomunicazione. Il potere di ordinare tali mezzi investigativi è attribuito esclusivamente al giudice istruttore sotto la sua autorità ed il suo controllo. Il legislatore ha distinto chiaramente le intercettazioni da altri atti che il giudice può disporre senza restrizioni, dettando condizioni assai rigide. Infatti è possibile ricorrervi solo in materia di crimini o delitti per i quali sia prevista una pena detentiva non inferiore a due anni e siano ritenute necessarie allo svolgimento delle indagini. La decisione non riveste carattere giurisdizionale, di conseguenza non deve essere motivata e non è suscettibile di ricorso.

La decisione deve essere espressa per iscritto e contenere tutti gli elementi di identificazione della linea da intercettare, la specificazione del reato che la motiva e la sua durata (art. 100-1). L'art. 100-2 stabilisce che la durata non può essere superiore a quattro mesi e la decisione può essere rinnovata alle stesse condizioni di forma e di tempo. I termini previsti trovano giustificazione nel fatto di evitare che la misura possa prolungarsi a tempo indeterminato sulla base della decisione iniziale, senza che il giudice ne controlli regolarmente i risultati e ne apprezzi l'utilità.

Ai sensi dell'articolo 100-3 il giudice istruttore o l'ufficiale di polizia giudiziaria da lui incaricato può richiedere, per l'installazione di un dispositivo di intercettazione, la collaborazione di un operatore qualificato che dipenda dal servizio pubblico di telecomunicazione o da un gestore autorizzato. Gli operatori sono obbligati al rispetto del segreto istruttorio e al segreto della corrispondenza, non possono rivelare l'esistenza delle intercettazioni e il contenuto della corrispondenza.

L'articolo 100-4 precisa le formalità relative alle operazioni di intercettazione e registrazione della corrispondenza di cui deve essere redatto un processo verbale che indichi la data e l'ora in cui è iniziata e terminata l'operazione. Le registrazioni devono poi essere sigillate.

La trascrizione delle registrazioni, ai sensi dell'articolo 100-5, è limitata alle parti della corrispondenza utili all'accertamento della verità e spetta al giudice istruttore o all'ufficiale di polizia giudiziaria da lui incaricato, con l'eventuale assistenza di un interprete, qualora le conversazioni siano in lingua straniera. Il verbale deve poi essere versato nel fascicolo.

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

L'articolo 100-7 pone dei limiti relativi alle persone oggetto delle intercettazioni: in primo luogo si esclude la possibilità di registrare le conversazioni sulla linea di un parlamentare se non ne sia stato informato il Presidente dell'Assemblea di appartenenza da parte del giudice istruttore. Tali limiti si applicano anche ai magistrati, per i quali è richiesto che ne sia informato il presidente o il procuratore generale della giurisdizione di appartenenza. Ispirandosi alle disposizioni dell'articolo 56-1 c.p.p. relative alle formalità applicabili in caso di perquisizione di uno studio di avvocato, l'articolo 100-7 precisa inoltre che il giudice istruttore deve informare il Presidente del consiglio dell'ordine qualora ritenga necessario disporre l'intercettazione della linea telefonica di un avvocato, ciò nel rispetto della regola della libertà di comunicazione tra l'inquisito e il suo difensore.

Con il decreto 2006-1405 del 17 novembre 2006[1] é stata istituita, presso il Ministero della giustizia, la Delegazione alle intercettazioni giudiziarie, organo sottoposto al Segretario generale del Ministero e diretto da un magistrato, cui è affidata la missione generale di razionalizzare in ambito interministeriale ed in termini di procedura, di mezzi tecnici e di costi, le intercettazioni e la raccolta di dati di traffico disposti dai magistrati. La sua competenza è di carattere tecnico, giuridico e finanziario.

Le intercettazioni di sicurezza

Le intercettazioni di sicurezza hanno carattere amministrativo, sono disposte dal Governo e sono di competenza della polizia amministrativa. La materia è regolata dalla già citata legge n. 646 del 1991, ampiamente modificata dalla legge 2004-669 relativa alle comunicazioni elettroniche e ai servizi di comunicazione audiovisiva.

Le intercettazioni di questo tipo sono sottoposte a limiti di legalità che ne garantiscono la trasparenza necessaria, assicurandone comunque l'efficacia. Rivestono carattere preventivo ed hanno lo scopo di raccogliere informazioni relative al loro campo di applicazione che riguarda la prevenzione degli attentati alla sicurezza nazionale, la salvaguardia di elementi essenziali al potenziale scientifico ed economico della Francia, la prevenzione del terrorismo, della criminalità organizzata e della ricostituzione dei gruppi combattenti e delle milizie private sciolti in applicazione della legge del 10 gennaio 1936.

La legge sottolinea il carattere eccezionale di tali intercettazioni (articolo 3) e prescrive una procedura molto rigorosa, nel rispetto dei principi costituzionali del segreto della corrispondenza, della libertà individuale e del diritto alla riservatezza. L'autorizzazione ad effettuare le intercettazioni deve essere accordata, con decisione scritta e motivata, dal Primo ministro o da una delle due persone cui abbia conferito una delega speciale (articolo 4). La domanda di autorizzazione deve essere formalizzata dal Ministro della difesa o dal Ministro dell'interno o dal Ministro competente delle dogane.

L'autorizzazione è concessa per una durata massima di quattro mesi e cessa di produrre effetti allo scadere di questo termine, può comunque essere rinnovata alle stesse condizioni di forma e di durata (articolo 6). Il numero di intercettazioni suscettibili di essere praticate simultaneamente è ripartito tra i tre ministeri competenti in base ad una decisione del Capo del governo (articolo 5).

La trascrizione delle registrazioni effettuate è limitata alle informazioni rilevanti ai fini di uno degli obiettivi indicati dalla legge. Di ognuna delle operazioni di intercettazione e di registrazione deve essere redatto un rapporto da cui risulti la data e l'ora di inizio e di fine dell'operazione. Le registrazioni devono essere distrutte entro un termine massimo di dieci giorni dalla data in cui sono state effettuate. Le trascrizioni delle intercettazioni devono essere distrutte quando la loro conservazione non risulti più indispensabile alla realizzazione dei fini per cui sono state disposte.

La legge del 1991 (articolo 13) ha istituito la Commissione nazionale di controllo delle intercettazioni di sicurezza quale organo di garanzia contro eventuali abusi del potere esecutivo. La Commissione è un'autorità amministrativa indipendente presieduta da una personalità designata, per sei anni, dal Presidente della Repubblica sulla base di una lista di quattro nomi proposta congiuntamente dal vicepresidente del Consiglio di Stato e dal primo presidente della Corte di Cassazione; essa comprende tra i suoi membri un deputato ed un senatore; la qualità di membro è incompatibile con incarichi di Governo; il mandato non è rinnovabile e non può essere concluso salvo dimissioni o su decisione della Commissione stessa.

Alla Commissione spetta il controllo della corretta applicazione della normativa da parte dell'esecutivo. Pertanto il Presidente è informato delle autorizzazioni concesse dal Primo ministro nel termine di 48 ore, e qualora ravvisi dubbi di legalità convoca la Commissione che è tenuta a pronunciarsi nei sette giorni successivi. La Commissione può inoltre procedere al controllo di qualsiasi intercettazione, di propria iniziativa o su reclamo di chiunque abbia un interesse diretto e personale. Nel caso in cui vengano rilevate irregolarità viene indirizzata al Capo del Governo, ed al Ministro interessato, una raccomandazione affinché sia interrotta l'intercettazione. Essa può informare il Procuratore della Repubblica delle eventuali infrazioni alla legge rilevate nella procedura di controllo.L'esigenza di trasparenza nella pratica delle intercettazioni è assicurata infine dalla pubblicazione del rapporto annuale che la Commissione di controllo presenta al Primo ministro[2].

GERMANIA

Il quadro normativo

Il segreto della corrispondenza e delle telecomunicazioni sono garantiti dall'articolo 10 della Legge fondamentale (*Grundgesetz*)[3]. Ai sensi di tale articolo il segreto della corrispondenza e così pure il segreto postale e delle telecomunicazioni sono inviolabili. Limitazioni possono essere stabilite solo con legge. Lo stesso articolo 10 prevede poi che nel caso in cui la limitazione sia finalizzata alla difesa dell'ordinamento costituzionale liberale e democratico o dell'esistenza o della sicurezza della Federazione o di un Land, la legge stessa può stabilire che la misura restrittiva non venga comunicata all'interessato e che il ricorso giurisdizionale sia sostituito da un esame da parte di organi istituiti dal Parlamento.

Nell'ambito delineato dalle previsioni costituzionali il legislatore federale ha adottato una serie di provvedimenti che regolamentano la materia delle intercettazioni nel settore delle telecomunicazioni:

- gli articoli 100a e 100b[4] del Codice di procedura penale (*Strafprozeßordnung - StPO*) disciplinano le intercettazioni nell'ambito di inchieste giudiziarie;
- la legge sulla limitazione del segreto epistolare, postale e delle telecomunicazioni(*Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses*)[5], c.d. legge sull'articolo 10 della costituzione (*G-10 Gesetz)*[6]del 26 giugno 2001, riguarda le intercettazioni che possono essere effettuate su richiesta dei servizi segreti federali;
- la parte terza del capitolo 2 (articoli da 23a a 23g)[7] della Legge sui servizi investigativi doganali (*Zollfahndungsdienstgesetz)****[8]*** del 16 agosto 2002, è dedicata alle intercettazioni delle telecomunicazioni e alle intercettazioni postali.

Infine, sulla base dell'articolo 110 della Legge federale sulle telecomunicazioni (*Telekommunikationsgesetz – TKG)****[9]*** e per l'applicazione delle misure previste nelle disposizioni sopra citate e nella normativa dei *Länder*, il Governo federale ha adottato un regolamento ministeriale (*Verordnung über die technische und organisatorische Umsetzung von Maßnahmen zur Überwachung der Telekommunikation - TKÜV)****[10]***in vigore dal 3 novembre 2005. Il decreto, che contiene essenzialmente disposizioni di natura procedurale, stabilisce i requisiti di carattere tecnico e organizzativo per l'attuazione delle

misure previste dalla legge in materia di controllo delle telecomunicazioni nei vari ambiti in cui possono essere autorizzate intercettazioni nei confronti di determinati individui (c.d. controllo individuale, *Individualkontrolle*, tipico delle inchieste giudiziarie) o senza riferimento a persone specifiche (c.d. controllo strategico, *strategische Kontrolle*, richiesto dai servizi di *intelligence*).

Tutte le norme sopra citate sono state di recente modificate con due interventi legislativi: la legge di riforma della disciplina sulle intercettazioni telefoniche e su altre misure investigative nascoste, nonché di attuazione della Direttiva 2006/24/CE del 21 dicembre 2007 (*Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG* - BGBl., I, S. 3198) e la modifica della normativa sui servizi investigativi doganali e di altre leggi del 12 giugno 2007 (*Gesetz zur Änderung des Zollfahndungsdienstgesetzes und anderer Gesetze* - BGBl., I, S. 1037). L'approvazione di una riforma della disciplina relativa alle intercettazioni nel settore delle telecomunicazioni è stata dettata, oltre che dalle innovazioni tecnologiche e dalle difficoltà evidenziate dalla prassi dell'azione penale nell'applicazione delle disposizioni vigenti in materia, dall'esigenza di conformarsi ad alcune sentenze del Tribunale costituzionale federale. In particolare, la sentenza del 27 luglio 2005 (BVerfGE 113, 348, 391) ha stabilito chiaramente che anche nell'ambito delle intercettazioni sono necessarie delle regole per la tutela della sfera intima della vita privata.

Le principali novità introdotte dalle nuove leggi hanno riguardato da un lato alcune sostanziali modifiche del regime delle intercettazioni disciplinato nel Codice di procedura penale; dall'altro, una serie di modifiche della Legge federale sulle telecomunicazioni in materia di rilevazione, memorizzazione, conservazione e cancellazione dei dati sul traffico telefonico. Con la nuova legge è stata infatti recepita, nell'ordinamento tedesco, la direttiva comunitaria n. 2006/24/CE del 15 marzo 2006 riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione.

Le intercettazioni nell'ambito di inchieste giudiziarie

In base alle disposizioni contenute nell'articolo 100a del Codice di procedura penale possono essere effettuate intercettazioni e registrazioni di conversazioni telefoniche nei confronti di una o più persone sospettate di aver commesso, in prima persona o in veste di complice, uno dei gravi reati elencati nello stesso articolo e sanzionati con una pena detentiva di almeno cinque anni. L'elenco dei reati comprende: l'attentato alla pace, l'alto tradimento e la minaccia dell'ordinamento democratico dello Stato e della sicurezza

esterna; reati contro l'ordine pubblico; l'istigazione e il concorso alla diserzione; l'attentato alla sicurezza delle truppe stazionate in Germania e appartenenti ad altri Stati membri dell'Alleanza atlantica; la falsificazione di denaro e titoli; l'abuso sessuale di minori e la diffusione della pornografia; l'omicidio e il genocidio; la rapina e l'estorsione; il traffico di armi da guerra e lo spaccio di stupefacenti. Con la modifica del 2007 sono state inserite nuove fattispecie tipiche della criminalità economica come la corruzione, la frode commerciale, il falso in bilancio, l'evasione fiscale, nonché crimini di guerra e contro l'umanità sanzionati nel Codice penale internazionale, la tratta di essere umani e ogni forma di diffusione di pronografia infantile.

L'intercettazione è consentita quando sussiste il sospetto di un tale reato. Il provvedimento è sussidiario. Il controllo è infatti ammissibile soltanto qualora la conduzione delle indagini e la perquisizione dell'abitazione della persona indagata risultino particolarmente complesse con altri strumenti e non offrano utili prospettive ai fini dell'esito delle indagini stesse.

L'ordinanza può adottarsi solo contro l'imputato e contro persone delle quali possa supporsi, in base a determinati elementi di fatto, che ricevano o trasmettano comunicazioni indirizzate o provenienti dall'imputato oppure nel caso in cui lo stesso imputato utilizzi la linea telefonica di tali persone.

Ai sensi dell'articolo 100b del Codice di procedura penale, come di recente modificato, le intercettazioni e le registrazioni di conversazioni telefoniche possono essere disposte soltanto dal tribunale su richiesta della procura o, in caso di pericolo imminente, dalla procura stessa. L'ordinanza sottoscritta dal procuratore cessa di avere effetto se non viene convalidata dal tribunale entro tre giorni lavorativi. L'ordinanza, emanata in forma scritta, deve contenere nome, indirizzo e numero telefonico della persona cui è diretta e stabilire con precisione la modalità, l'entità e la durata delle intercettazioni. La validità dell'ordinanza è di tre mesi al massimo. Il termine può essere prorogato soltanto per altri tre mesi purché sussistano i presupposti indicati nell'art. 100a.

Ogni anno i *Länder* e il Procuratore generale federale riferiscono all'Ufficio federale della giustizia (*Bundesamt für Justiz*) in merito a tutte le procedure di intercettazione disposte ai sensi dell'articolo 100a. L'Ufficio federale della giustizia elabora poi, a fini statistici, un prospetto riepilogativo che viene pubblicato sul suo sito Internet. Anche nel caso di inchieste giudiziarie relative a gravi reati, non sono ammesse ingerenze nella vita privata. A tale proposito le nuove disposizioni (art. 100a, comma 4) contengono un esplicito divieto di rilevare ed utilizzare i contenuti di comunicazioni afferenti la sfera intima di una persona. Se durante una conversazione telefonica si parla di sentimenti particolarmente intimi e di riflessioni molto personali, non è consentita l'intercettazione della telefonata. La registrazione deve essere immediatamente cancellata e le informazioni

eventualmente ottenute non potranno essere utilizzate nel corso di un procedimento penale.

Per quanto concerne i soggetti obbligati al segreto professionale (ad esempio medici, giornalisti, avvocati, notai) vige il diritto di non deporre (*Zeugnisverweigerungsrecht*) nel corso di un interrogatorio ai sensi dell'art. 53 del Codice di procedura penale. La loro particolare tutela è stata estesa, con le recenti modifiche del 2007, a tutte le misure investigative e risulta quindi notevolmente rafforzata. Continuano a sussistere, senza limiti, anche le disposizioni che prevedono il divieto di confisca (art. 98) e il divieto di sorveglianza dell'abitazione (art. 100c, comma 6) di tali soggetti. Una protezione particolare è assicurata dalla legge ai padri spirituali, ai difensori penalisti e ai membri del Parlamento.

In attuazione della direttiva comunitaria n. 2006/24/CE è fatto obbligo ai fornitori di servizi di comunicazione elettronica accessibili al pubblico, o di una rete pubblica di comunicazione, di immagazzinare dati relativi al traffico e di conservarli per un periodo di sei mesi ai fini eventuali dell'azione penale. Polizia e procura dello Stato potranno accedere a tali dati soltanto con il consenso del tribunale, nell'ambito di una inchiesta giudiziaria per l'accertamento di una fattispecie concreta di reato. Nella decisione del giudice deve essere stabilito con precisione quali dati l'impresa di telecomunicazione deve selezionare e trasmettere all'autorità giudiziaria.

Chiunque fornisca a scopo commerciale servizi di telecomunicazione è obbligato, sulla base del contenuto dell'ordinanza, a consentire al giudice, al procuratore e agli investigatori della polizia l'intercettazione e la registrazione delle telefonate.

Nel caso in cui vengano meno i presupposti che sono alla base dell'emanazione dell'ordinanza, le intercettazioni devono cessare immediatamente e di ciò è data comunicazione al giudice e ai fornitori dei servizi di telecomunicazioni interessati. I dati sensibili e le informazioni raccolte possono essere utilizzate in altri procedimenti penali a fini di prova soltanto nella misura in cui emergano fatti e cognizioni necessari a far luce su uno dei reati elencati nel precedente art. 100a. Viceversa, se la documentazione ottenuta non è più necessaria all'azione penale, deve essere immediatamente distrutta sotto il controllo della procura.

Le intercettazioni a fini di sicurezza

La legge sui limiti all'articolo 10 della Legge fondamentale consente alle autorità di tutela costituzionale (*Verfassungschutzbehörden*) e ai servizi segreti (*Militärischer Abschirmdienst* e *Bundesnachrichtendienst*) di effettuare intercettazioni nei confronti di persone specifiche (*Beschränkungen in Einzelfällen*) nel caso in cui vi siano fondati

sospetti circa la progettazione o il compimento di alcuni dei reati che figurano anche nell'elenco dell'art. 100a del codice di procedura penale, oppure nei confronti di una serie di persone indeterminate a fini strategici per la tutela della sicurezza nazionale. Per questo primo tipo di controllo relativo a singoli casi (disciplinato dagli articoli 3 e 4 della legge stessa) si applicano disposizioni analoghe a quelle contenute nel Codice di procedura penale.

Alle cd. limitazioni strategiche (*strategische Beschränkungen*) è invece dedicata la Parte terza della legge, in particolare l'articolo 5, che specifica i casi in cui è necessario ottenere informazioni volte a sventare situazioni di grave pericolo per lo Stato, in primo luogo attacchi armati o attentati terroristici. Si tratta di provvedimenti rivolti non a soggetti singoli, bensì ad una serie o gruppo di persone non determinate individualmente. Tali provvedimenti restano segreti e non sono sottoposti al controllo di un giudice ma di un Comitato parlamentare di controllo (*Parlamentarisches Kontrollgremiums*). L'ordine di attivare i controlli è emanato, su richiesta dei servizi di *intelligence*, dal Ministro federale dell'Interno con la necessaria approvazione del Comitato di controllo parlamentare. Sull'ammissibilità e la necessità delle limitazioni disposte con l'ordinanza ministeriale decide poi un apposito organo istituito dall'art. 15 della legge stessa, la c.d. *G 10-Kommission*, i cui componenti (il Presidente, tre membri effettivi e quattro supplenti) sono nominati dal Comitato di controllo parlamentare per tutta la durata della legislatura. Le competenze della Commissione, che si riunisce in seduta segreta almeno una volta al mese, si estendono al controllo di tutte le fasi relative al rilevamento, all'elaborazione e all'utilizzo dei dati personali raccolti dai servizi di sicurezza sulla base delle misure restrittive autorizzate. Spetta inoltre alla Commissione decidere, dopo l'archiviazione delle misure, in merito all'opportunità di darne comunicazione alle persone interessate (art. 12).

Le intercettazioni preventive nelle telecomunicazioni e le intercettazioni postali

La Parte terza del Capitolo 2 della legge sui servizi investigativi doganali è dedicata alle intercettazioni preventive delle telecomunicazioni e postali (artt. dal 23a al 23g)[11] nel caso in cui vi sia il sospetto che si stiano per compiere reati in violazione della legge sul controllo delle armi da guerra (*Gesetz über di Kontrolle von Kriegswaffen*)[12], con particolare riferimento alla elaborazione, produzione e commercio di armi atomiche, biologiche, chimiche e di mine antipersona.

La legge sui servizi investigativi doganali, entrata in vigore nel 2002 ha subito una rilevante modifica ad opera della legge del 14 giugno 2007. A seguito di alcune sentenze pronunciate dal Tribunale costituzionale federale in relazione a questa materia si erano

resi infatti necessari diversi adeguamenti normativi. Al fine di adeguare la legge alla decisione del Tribunale costituzionale federale del 27 luglio 2005 (1 BvR 668/04), con cui sono stati precisati i limiti delle ingerenze determinate da misure investigative, al comma 4a dell'art. 23a sono state inserite alcune disposizioni finalizzate alla tutela della vita privata: pertanto, nel caso in cui vengano registrati dati che attengono alla vita privata, tali dati non sono comunque utilizzabili.

In considerazione di un'altra sentenza del Tribunale costituzionale federale (1 BvR 2378/98 del 3 marzo 2004) sulla sorveglianza e il controllo dell'abitazione, i nuovi artt. 22a e 32a della *Zollfahndungsdienstgesetz* stabiliscono che, nel caso in cui l'Ufficio doganale anticrimine e gli altri servizi investigativi doganali esercitino i poteri attribuitigli dalla legge per la prevenzione e la persecuzione di reati penali o per la scoperta di crimini sconosciuti, le persone incaricate possono utilizzare mezzi tecnici per la videoregistrazione e l'intercettazione di parole non dette in pubblico all'interno di abitazioni, nella misura in cui ciò sia indispensabile alla difesa da pericoli per il corpo, per la vita o per la libertà. Qualora venga coinvolto il nucleo della vita privata di una persona, la misura investigativa intrapresa deve essere interrotta a patto che sia possibile senza pericolo per la persona incaricata della sorveglianza.

L'art. 23g riguarda in modo specifico la rilevazione dei dati relativi all'utilizzo di servizi di telecomunicazione (*Verkehrsdaten*), cioè il traffico telefonico, sia fisso che mobile, e la navigazione in Internet. Nel caso in cui vi siano fondati sospetti che qualcuno stia preparando un crimine che metta a repentaglio la sicurezza e l'ordine pubblico, l'Ufficio doganale anticrimine può ottenere la rilevazione dei dati relativi al traffico telefonico anche senza che ne sia a conoscenza la persona interessata. Di regola è necessaria un'autorizzazione del giudice, ma in caso di pericolo imminente l'ordine può essere disposto anche tramite il Ministero federale delle finanze. Se la successiva convalida da parte del tribunale non avviene entro tre giorni, la misura intrapresa cessa ogni effetto. L'ordinanza ha una scadenza massima di tre mesi, ma è tuttavia possibile prorogarla fino ad altri tre mesi purché sussistano ancora i presupposti originari e tale misura sia da ritenersi ragionevole. In base al disposto dell'ordinanza i servizi di telecomunicazione hanno l'obbligo di consentire all'Ufficio doganale anticrimine il rilevamento del traffico e di fornirgli tutte le informazioni necessarie.

REGNO UNITO

Il quadro normativo

La principale fonte normativa in materia di intercettazioni è costituita dal *Regulation of Investigatory Powers Act* del 2000 (RIPA)[13], con cui il legislatore, mettendo mano alla precedente regolamentazione del 1985, ha compiuto una organica revisione dei poteri investigativi delle autorità inquirenti e delle forze di polizia, resasi necessaria in ragione dell'evoluzione tecnologica e, soprattutto, della diffusione delle comunicazioni elettroniche e dei dispositivi di crittografia.

La legge del 2000 disciplina, in particolare, le attività di investigazione il cui esercizio contempli l'intercettazione delle comunicazioni, l'acquisizione dei dati relativi al traffico telefonico, la decrittazione dei dati, il ricorso ad agenti ed informatori. Essa delinea, d'altra parte, un quadro di garanzie attraverso la delimitazione delle finalità per il legittimo uso di questi strumenti investigativi, l'individuazione dei soggetti abilitati ad avvalersene, la previsione di appositi procedimenti di autorizzazione, il conferimento alla magistratura di compiti di supervisione indipendente e, infine, il riconoscimento alle persone interessate di un diritto di opposizione, a seconda dei casi, all'effettuazione o alla prosecuzione delle attività suddette.

Merita subito osservare come tale bilanciamento di interessi, perseguito dal legislatore nell'intento di far salvi nella loro integrità i principi di tutela dei diritti fondamentali sanciti dallo *Human Rights Act* del 1998, sia divenuto, negli anni più recenti e in ragione del drammatico accentuarsi della minaccia del terrorismo internazionale, tema assai controverso e dibattuto in sede politica e presso l'opinione pubblica. Mentre il grado di compatibilità di diritti fondamentali - come quello di espressione e alla riservatezza - con le necessità radicate nella pubblica sicurezza - quali la prevenzione e repressione delle attività terroristiche - è argomento ancor oggi ricorrente e talora motivo di proposte variamente restrittive della sfera dei diritti (ispirate dalla convinzione che le tutele previste dallo *Human Rights Act* siano d'impaccio ad una efficace contrasto del terrorismo[14]), la concreta applicazione della disciplina, e l'obiettiva complessità degli ambiti regolati, hanno intanto richiesto che essa si ramificasse nella cospicua serie di *Statutory Instruments* adottati dal 2000 ad oggi[15], e che taluni profili specifici fossero affidati, secondo un tratto caratteristico dell'ordinamento britannico, alle più duttili previsioni di codici di condotta. Tra questi vengono in rilievo il codice specificamente adottato, il 24 novembre 2005, in attuazione della legge medesima, nonché, per i profili generali, il codice sulla conservazione dei dati delle comunicazioni (*data retention*), intervenuto successivamente a corredo della legislazione anti-terrorismo emanata dal 2001.

Sia la normativa di dettaglio che il codice di condotta sulle intercettazioni sono riferiti ad un settore particolare delle attività, tra loro correlate, nelle quali si esplicano i poteri investigativi disciplinati dalla legge del 2000. Oltre alle *interceptions*, il RIPA disciplina infatti la *directed surveillance*, definita come "la sorveglianza connotata da segretezza (*under cover*) ma non intrusiva", e la *intrusive surveillance*, la quale comporta l'accesso in aree o in veicoli di proprietà privata od anche la collocazione di dispositivi di ascolto. Occorre segnalare che anche per queste attività, diverse dalle intercettazioni - secondo il criterio adottato dal legislatore - ma connotate da una certa omogeneità quanto ai principi applicabili, è prevista dalla legge l'adozione di codici di condotta[16].

La disciplina delle intercettazioni

Disciplinate dalle disposizioni raccolte nel RIPA (nel primo titolo della prima parte), le intercettazioni delle comunicazioni possono generalmente essere effettuate, con riguardo al mezzo postale o ai sistemi di telecomunicazione, da parte delle autorità preposte alla tutela dell'ordine pubblico e dei servizi di sicurezza previa autorizzazione resa dall'autorità ministeriale (di norma, lo *Home Office*). Tale autorizzazione (*warrant*), come prescrive la legge, è rilasciata purché siano sussistenti i fondamentali requisiti della necessità e della proporzionalità. E' pertanto necessario che l'autorità richiedente comprovi che le intercettazioni da effettuare siano effettivamente necessarie a proteggere la sicurezza nazionale, ad individuare o a prevenire attività criminali di particolare gravità, o a salvaguardare la ricchezza economica del Paese; e che i benefici derivanti dalle attività per le quali è richiesta autorizzazione siano tali da giustificare l'intrusione nella sfera privata dei singoli e da evitare ogni altra interferenza se non quella strettamente necessaria allo scopo. In sede di autorizzazione occorre inoltre valutare se le informazioni che ci si propone di acquisire mediante le intercettazioni non possano essere ottenute in altro modo.

Agli operatori di sistemi di telecomunicazione (*Public Telecommunication Operators*) è richiesto, d'altra parte, di provvedere affinché i loro sistemi siano tecnicamente configurati in modo da essere accessibili alle intercettazioni legittimamente effettuate.

Le informazioni così ottenute non hanno, tuttavia, valore probatorio e, salvo alcune eccezioni, non possono generalmente essere utilizzate come prove nei procedimenti giurisdizionali (art. 17 della legge). Questo divieto, benché ritenuto pienamente conforme all'art. 6 della Convenzione europea dei diritti dell'uomo e coerente con il principio della condizione di parità tra accusa e difesa tradizionalmente tipico del sistema penale britannico, è stato, nel 2003, sottoposto a revisione su impulso del Primo Ministro, senza

però che, ad esito delle nuove valutazioni, si giungesse alla scelta di modificare la disciplina. Si è infatti ritenuto che i rischi inerenti alla accessibilità degli atti processuali, e dunque anche delle intercettazioni e dei criteri con i quali esse sono poste in essere, avrebbero superato i vantaggi derivanti dal valore probatorio ad esse assegnato, in quanto la pubblicità delle tecniche investigative avrebbe indebolito l'azione repressiva dello Stato nei confronti della criminalità, specialmente di tipo terroristico[17].

Le Autorità di vigilanza e di riesame

Sulla corretta applicazione delle disposizioni del RIPA in materia di intercettazioni è preposto a vigilare lo *Interception of Communications Commissioner*, autorità monocratica istituita dalla medesima legge (art. 57) al fine di sottoporre ad uno scrutinio indipendente l'esercizio di poteri certamente invasivi della libertà personale e della sfera privata. Nominato dal Primo Ministro tra persone che abbiano rivestito cariche nell'alta magistratura, il *Commissioner* esercita, in particolare, compiti di controllo sul rilascio delle autorizzazioni (i già menzionati *warrants*) e sulla sussistenza dei presupposti prescritti della legge, riferendone al Governo con un rapporto pubblicato ogni anno[18].

Il RIPA ha altresì istituito (con le disposizioni raccolte nella quarta parte del testo normativo, e al fine di una razionalizzazione di competenze precedentemente distribuite tra diversi organismi[19]) un'autorità paragiurisdizionale indipendente preposta all'esame dei ricorsi e dei reclami presentati dai soggetti passivi delle intercettazioni: l'*Investigatory Powers Tribunal* (IPT)[20], le cui regole di funzionamento hanno fonte in un'apposita legge[21], è composto da otto membri di nomina regia provenienti dalle professioni forensi, i quali durano in carica cinque anni e possono essere confermati[22].

I codici di condotta

Il quadro delle fonti normative rilevanti per la materia in esame è integrato principalmente da due codici di condotta, l'uno dedicato alle intercettazioni, l'altro, intervenuto successivamente all'approvazione dello *Anti-Terrorism, Crime and Security Act* del 2001, agli aspetti della conservazione dei dati inerenti alle stesse comunicazioni.

Il primo codice, redatto secondo le previsioni del RIPA (e denominato *Interception of Communication Code of Practice*[23]), individua in via generale, al secondo paragrafo, le autorità abilitate al rilascio di autorizzazioni con riferimento alle attività di intercettazione; richiama i requisiti di necessità e di proporzionalità la cui sussistenza deve essere considerata in sede di rilascio del *warrant*; ne fissa la validità per

un periodo di tre mesi, rinnovabile per altri tre o sei mesi a seconda che l'attività investigativa riguardi la criminalità organizzata (*serious crime*) oppure la sicurezza dello Stato; pone un obbligo di cooperazione ed assistenza (*reasonable assistance*) sugli operatori di sistemi di telecomunicazione, su richiesta dell'autorità autorizzata alle intercettazioni, nonché di garantire, sul piano della configurazione tecnica dei sistemi da loro gestiti, un livello di "permeabilità" rispetto alle attività di intercettazione legittimamente effettuate (*provision of intercept capability*).

E' dato altresì rilievo puntuale, nel terzo paragrafo del codice, agli aspetti relativi alla violazione della riservatezza di individui diversi dai soggetti passivi delle intercettazioni autorizzate, soprattutto quando le informazioni acquisite sul loro conto riguardino dati sensibili o la cui comunicazione abbia luogo nel quadro di attività protette dal segreto professionale (giornalisti, medici, ministri del culto). In sede di rilascio del *warrant* devono, pertanto, essere valutati i rischi inerenti alla possibile violazione della *privacy* di terzi (*collateral intrusion*) o alla natura confidenziale delle informazioni comunicate (*confidential information*).

Dopo aver disciplinato in dettaglio, nel quarto e nel quinto paragrafo, il procedimento di rilascio dei *warrants* e sul loro rinnovo, il codice detta nel sesto paragrafo norme di salvaguardia relativamente all'uso delle informazioni raccolte, di cui deve essere garantita la conformità ai termini indicati nei *warrants* e alle prescrizioni generali del *Commissioner*. Il materiale tratto dalle intercettazioni non può infatti essere diffuso, riprodotto o conservato se non nei limiti delle finalità per le quali le intercettazioni medesime sono state autorizzate, oltre che per alcuni scopi di rilevante interesse pubblico individuati dall'art. 15 della legge (ad esempio, la tutela della sicurezza pubblica o del benessere economico del Paese, l'espletamento dei compiti istituzionali delle autorità ministeriali e del *Commissioner* o del *Tribunal*); raggiunte dette finalità il materiale suddetto, la cui diffusione ha carattere circoscritto ed è soggetta a particolari misure di sicurezza, deve essere distrutto.

Il codice affronta inoltre, nel settimo paragrafo, il delicato profilo della rilevanza processuale delle intercettazioni, e in particolare della loro accessibilità da parte del magistrato titolare della pubblica accusa e dell'autorità giudicante.

Come si è anticipato, gli interventi legislativi con cui si è inteso far fronte, a partire dal 2001, alla rinnovata minaccia del terrorismo internazionale hanno avuto ricadute anche sul piano dei sistemi di comunicazione. Nuove regole sulla doverosa conservazione dei dati da parte degli operatori di telecomunicazione per finalità di prevenzione del terrorismo, nella ricerca di un non facile bilanciamento con le norme vigenti in materia di protezione dei diritti dell'uomo e di trattamento dei dati personali, sono state delineate dalla legge già menzionata del 2001 e dettate in dettaglio dall'apposito

codice di condotta sulla *retention of communications data*[24]. Per la materia in esame, e laddove le attività criminose oggetto di indagine siano contemplate dalla legge richiamata, devono pertanto segnalarsi le previsioni del codice concernenti la tipologia dei dati suscettibili di essere conservati (in deroga ai principi che ne richiederebbero altrimenti la distruzione una volta esaurito lo scopo della loro raccolta) e la durata della loro conservazione.

SPAGNA

Il quadro normativo

L'articolo 18.3 della Costituzione spagnola proclama che "E' garantito il segreto delle comunicazioni e, in specie, di quelle postali, telegrafiche e telefoniche, salvo decisione giudiziale."

A fronte di tale diritto fondamentale, il Codice di procedura penale (*Ley de enjuiciamiento criminal*), a seguito delle modifiche apportate nel 1988, contiene all'articolo 579 delle sintetiche disposizioni relative alla possibile limitazione del suddetto diritto. In particolare (comma 1) viene consentito al giudice di accordare il sequestro della corrispondenza privata, postale e telegrafica di una persona indagata, se vi siano "indizi di ottenere in tali modi la scoperta o la conferma di alcun fatto o circostanza importante del procedimento"; lo stesso può avvenire, mediante risoluzione motivata, per l'intercettazione delle comunicazioni telefoniche dell'interessato (comma 2), sempre in presenza dei medesimi indizi. Il codice prevede inoltre (comma 3) che le comunicazioni possano essere tenute sotto osservazione per un periodo di tre mesi, prorogabile per uguali periodi di tempo, sempre mediante risoluzione motivata del giudice, per "le persone per le quali vi siano indizi di responsabilità penale, così come per le comunicazioni delle quali esse si servano per la realizzazione dei loro scopi criminali". E' disposto infine (comma 4) che, in caso di urgenza, quando le indagini si attuino per l'accertamento di reati collegati all'attività di bande armate o di elementi terroristi, l'adozione della misura prevista al comma 3 possa essere deliberata dal Ministro dell'Interno o, in sua vece, dal Direttore della Sicurezza dello Stato, comunicando le motivazioni per iscritto al giudice competente, che confermerà o revocherà tale decisione entro 72 ore.

La giurisprudenza in tema di intercettazioni telefoniche

La legislazione spagnola non contiene altre disposizioni in materia di intercettazioni telefoniche e non specifica i presupposti e i requisiti per l'adozione di una risoluzione valida né per l'accertamento degli indizi richiesti dalla legge.

E' stata quindi la giurisprudenza del Tribunale Supremo e del Tribunale Costituzionale a porre alcuni principi fondamentali ed a precisare i concetti espressi dal legislatore.

In primo luogo è in alcune sentenze del Tribunale Supremo che compare la definizione di "intercettazione telefonica" (*intervención telefónica*),[25] intesa come "misura strumentale che presuppone una restrizione del diritto fondamentale al segreto delle comunicazioni e che è ordinata dal giudice istruttore ... al fine di captare il contenuto delle conversazioni per l'indagine di delitti precisi e per l'ottenimento, in caso, di determinati elementi probatori". Si tratta perciò di un "mezzo" il cui fine non è il semplice ascolto delle conversazioni ma la scoperta della commissione di un reato e dei suoi autori e l'ottenimento di elementi probatori da poter utilizzare in una successiva sede processuale. E' quindi indispensabile la decisione di un organo giudiziario per la limitazione di un diritto fondamentale garantito dalla Costituzione, che non può essere autorizzata da alcun organo amministrativo (polizia o forze di pubblica sicurezza), con l'eccezione temporanea del disposto al comma 4 dell'articolo 579

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

Si tratta di un principio che si applica con riferimento a tutti i diritti fondamentali[26] e che implica che ogni decisione limitativa di qualunque dei suddetti diritti debba essere adeguatamente argomentata, con motivazioni di fatto e di diritto che potranno essere successivamente valutate dal soggetto interessato, nell'esercizio del suo diritto di difesa, al fine di giudicare la proporzionalità tra la restrizione al diritto e la ragione che l'ha determinata.[27]

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

Dovrà quindi essere esaminato caso per caso dal giudice competente ed è compito dell'organo che richiede l'autorizzazione all'uso delle intercettazioni telefoniche (in genere le forze di polizia) fornire dati obiettivi e non semplici supposizioni o

congetture; è stato precisato che la decisione del giudice va comunque valutata in una prospettiva *ex ante*, con ponderazione degli elementi esistenti al momento della richiesta, e non deve essere giudicata *ex post*, cioè con giustificazione a posteriori, a seguito dei risultati ottenuti, o meno, con l'uso delle intercettazioni telefoniche.[28]

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

Il giudice istruttore, dopo la sua decisione, ha inoltre il dovere di seguire lo svolgimento delle attività di intercettazione, vigilando affinché la restrizione del diritto fondamentale resti comunque nei limiti costituzionali.[29]

In concreto sono stati poi precisati dalla giurisprudenza alcuni aspetti specifici relativi allo svolgimento delle attività di intercettazione, tra i quali vi è l'obbligo di consegnare al giudice le registrazioni originali ed in formato integrale,[30] con connessa esigenza di trascrizione integrale del contenuto delle registrazioni stesse, in modo da evitare "selezioni" o "tagli" preventivi da parte delle autorità di polizia.[31] Altro elemento imprescindibile, basato sul diritto alla difesa della persona indagata, consiste nel dovere di porre a conoscenza dell'interessato tutto il contenuto delle intercettazioni, nel termine massimo di 10 giorni prima della conclusione delle indagini preliminari, stabilito dall'articolo 302 del Codice di procedura penale, e di dar luogo ad un'audizione del soggetto stesso (*audición contradictoria*), innanzi al giudice, prima della conclusione di questa fase del procedimento.

Un'ultima importante questione, affrontata sia dal Tribunale Spremo che dal Tribunale Costituzionale, è quella delle conseguenze giuridiche di un'attività di intercettazione effettuata in modo illecito, cioè in violazione a quanto disposto dalla legge o dalla giurisprudenza consolidata, con riferimento alle prove della commissione di un reato eventualmente ottenute. L'orientamento dominante è quello della verifica se esista, o meno, una causalità diretta ed una connessione esclusiva tra l'intercettazione illecita e la prova (o le prove) risultanti a carico dell'indagato; si tratta di un concetto denominato "connessione di antigiuridicità" (*conexión de antijuridicidad*).[32] In sostanza occorre accertare, caso per caso, se le prove risultanti non avrebbero potuto essere ottenute senza l'intercettazione illecita, da considerarsi quindi come loro unica fonte di generazione,

oppure se queste godano di una certa indipendenza, nel senso che l'intercettazione non costituisce la loro unica fonte.[33]

In conclusione va segnalato che anche l'assenza di una normativa più dettagliata sugli aspetti procedurali menzionati è stata oggetto di critiche da parte dei giudici, che hanno censurato le lacune esistenti nelle disposizioni vigenti, invitando il legislatore ad approvare al più presto una normativa più adeguata in materia.[34]

Documentazione

FRANCIA

Code de procedure penale

(Partie Législative)

Sous-section II

Des interceptions de correspondances émises par la voie des télécommunications

Article 100

(Loi nº 85-1407 du 30 décembre 1985 art. 9 et art. 94 Journal Officiel du 31 décembre 1985 en vigueur le 1er février 1986)

(Loi nº 91-646 du 10 juillet 1991 art. 2 Journal Officiel du 13 juillet 1991 en vigueur le 1er octobre 1991)

En matière criminelle et en matière correctionnelle, si la peine encourue est égale ou supérieure à deux ans d'emprisonnement, le juge d'instruction peut, lorsque les nécessités de l'information l'exigent, prescrire l'interception, l'enregistrement et la transcription de correspondances émises par la voie des télécommunications. Ces opérations sont effectuées sous son autorité et son contrôle.

La décision d'interception est écrite. Elle n'a pas de caractère juridictionnel et n'est susceptible d'aucun recours.

Article 100-1

(inséré par Loi nº 91-646 du 10 juillet 1991 art. 2 Journal Officiel du 13 juillet 1991 en vigueur le 1er octobre 1991)

La décision prise en application de l'article 100 doit comporter tous les éléments d'identification de la liaison à intercepter, l'infraction qui motive le recours à l'interception ainsi que la durée de celle-ci.

Article 100-2

(inséré par Loi nº 91-646 du 10 juillet 1991 art. 2 Journal Officiel du 13 juillet 1991 en vigueur le 1er octobre 1991)

Cette décision est prise pour une durée maximum de quatre mois. Elle ne peut être renouvelée que dans les mêmes conditions de forme et de durée.

Article 100-3

(inséré par Loi nº 91-646 du 10 juillet 1991 art. 2 Journal Officiel du 13 juillet 1991 en vigueur le 1er octobre 1991)

Le juge d'instruction ou l'officier de police judiciaire commis par lui peut requérir tout agent qualifié d'un service ou organisme placé sous l'autorité ou la tutelle du ministre chargé des télécommunications ou tout agent qualifié d'un exploitant de réseau ou fournisseur de services de télécommunications autorisé, en vue de procéder à l'installation d'un dispositif d'interception.

Article 100-4

(inséré par Loi nº 91-646 du 10 juillet 1991 art. 2 Journal Officiel du 13 juillet 1991 en vigueur le 1er octobre 1991)

Le juge d'instruction ou l'officier de police judiciaire commis par lui dresse procès-verbal de chacune des opérations d'interception et d'enregistrement. Ce procès-verbal mentionne la date et l'heure auxquelles l'opération a commencé et celles auxquelles elle s'est terminée.
Les enregistrements sont placés sous scellés fermés.

Article 100-5

(Loi nº 91-646 du 10 juillet 1991 art. 2 Journal Officiel du 13 juillet 1991 en vigueur le 1er octobre 1991)

(Loi nº 2005-1549 du 12 décembre 2005 art. 38 Journal Officiel du 13 décembre 2005)

Le juge d'instruction ou l'officier de police judiciaire commis par lui transcrit la correspondance utile à la manifestation de la vérité. Il en est dressé procès-verbal. Cette transcription est versée au dossier.

Les correspondances en langue étrangère sont transcrites en français avec l'assistance d'un interprète requis à cette fin.

A peine de nullité, ne peuvent être transcrites les correspondances avec un avocat relevant de l'exercice des droits de la défense.

Article 100-6

(inséré par Loi nº 91-646 du 10 juillet 1991 art. 2 Journal Officiel du 13 juillet 1991 en vigueur le 1er octobre 1991)

Les enregistrements sont détruits, à la diligence du procureur de la République ou du procureur général, à l'expiration du délai de prescription de l'action publique.
Il est dressé procès-verbal de l'opération de destruction.

Article 100-7

(Loi nº 91-646 du 10 juillet 1991 art. 2 Journal Officiel du 13 juillet 1991 en vigueur le 1er octobre 1991)

(Loi nº 93-1013 du 24 août 1993 art. 20 Journal Officiel du 25 août 1993 en vigueur le 2 septembre 1993)

(Loi nº 95-125 du 8 février 1995 art. 50 Journal Officiel du 9 février 1995)

(Loi nº 2004-204 du 9 mars 2004 art. 5 Journal Officiel du 10 mars 2004)

Aucune interception ne peut avoir lieu sur la ligne d'un député ou d'un sénateur sans que le président de l'assemblée à laquelle il appartient en soit informé par le juge d'instruction.

Aucune interception ne peut avoir lieu sur une ligne dépendant du cabinet d'un avocat ou de son domicile sans que le bâtonnier en soit informé par le juge d'instruction.

Aucune interception ne peut avoir lieu sur une ligne dépendant du cabinet d'un magistrat ou de son domicile sans que le premier président ou le procureur général de la juridiction où il réside en soit informé.

Les formalités prévues par le présent article sont prescrites à peine de nullité.

Loi n° 91-646 du 10 juillet 1991

Loi relative au secret des correspondances émises par la voie des communications électroniques.

version consolidée au 24 janvier 2006

[. . .]

TITRE II : Des interceptions de sécurité.

Article 3

Modifié par Loi n°2004-669 du 9 juillet 2004 art. 125 (JORF 10 juillet 2004).

Peuvent être autorisées, à titre exceptionnel, dans les conditions prévues par l'article 4, les interceptions de correspondances émises par la voie des communications électroniques ayant pour objet de rechercher des renseignements intéressant la sécurité nationale, la sauvegarde des éléments essentiels du potentiel scientifique et économique de la France, ou la prévention du terrorisme, de la criminalité et de la délinquance organisées et de la reconstitution ou du maintien de groupements dissous en application de la loi du 10 janvier 1936 sur les groupes de combat et les milices privées.

Article 4

Modifié par Loi n°2006-64 du 23 janvier 2006 art. 6 III (JORF 24 janvier 2006).

L'autorisation est accordée par décision écrite et motivée du Premier ministre ou de l'une des deux personnes spécialement déléguées par lui. Elle est donnée sur proposition écrite et motivée du ministre de la défense, du ministre de l'intérieur ou du ministre chargé des douanes, ou de l'une des deux personnes que chacun d'eux aura spécialement déléguées.

Le Premier ministre organise la centralisation de l'exécution des interceptions autorisées.

Article 5

Modifié par Loi n°2004-669 du 9 juillet 2004 art. 125 (JORF 10 juillet 2004).

Le nombre maximum des interceptions susceptibles d'être pratiquées simultanément en application de l'article 4 est arrêté par le Premier ministre.

La décision fixant ce contingent et sa répartition entre les ministères mentionnés à l'article 4 est portée sans délai à la connaissance de la Commission nationale de contrôle des interceptions de sécurité.

Article 6

Modifié par Loi n°2004-669 du 9 juillet 2004 art. 125 (JORF 10 juillet 2004).

L'autorisation mentionnée à l'article 3 est donnée pour une durée maximum de quatre mois. Elle cesse de plein droit de produire effet à l'expiration de ce délai. Elle ne peut être renouvelée que dans les mêmes conditions de forme et de durée.

NOTA : Loi 2006-64 du 23 janvier 2006 art. 32 : Les dispositions de l'article 6 sont en vigueur jusqu'au 31 décembre 2008.

Article 7

Modifié par Loi n°2004-669 du 9 juillet 2004 art. 125 (JORF 10 juillet 2004).

Dans les correspondances interceptées, seuls les renseignements en relation avec l'un des objectifs énumérés à l'article 3 peuvent faire l'objet d'une transcription.

Cette transcription est effectuée par les personnels habilités.

Article 8

Modifié par Loi n°2004-669 du 9 juillet 2004 art. 125 (JORF 10 juillet 2004).

Il est établi, sous l'autorité du Premier ministre, un relevé de chacune des opérations d'interception et d'enregistrement. Ce relevé mentionne la date et l'heure auxquelles elle a commencé et celles auxquelles elle s'est terminée.

Article 9

Modifié par Loi n°2004-669 du 9 juillet 2004 art. 125 (JORF 10 juillet 2004).

L'enregistrement est détruit sous l'autorité du Premier ministre, à l'expiration d'un délai de dix jours au plus tard à compter de la date à laquelle il a été effectué.

Il est dressé procès-verbal de cette opération.

Article 10

Modifié par Loi n°2004-669 du 9 juillet 2004 art. 125 (JORF 10 juillet 2004).

Sans préjudice de l'application du deuxième alinéa de l'article 40 du code de procédure pénale, les renseignements recueillis ne peuvent servir à d'autres fins que celles mentionnées à l'article 3.

Article 11

Modifié par Loi n°2004-669 du 9 juillet 2004 art. 125 (JORF 10 juillet 2004).

Les opérations matérielles nécessaires à la mise en place des interceptions dans les locaux et installations des services ou organismes placés sous l'autorité ou la tutelle du ministre chargé des communications électroniques ou des exploitants de réseaux ou fournisseurs de services de télécommunications ne peuvent être effectuées que sur ordre du ministre chargé des communications électroniques ou sur ordre de la personne spécialement déléguée par lui, par des agents qualifiés de ces services, organismes, exploitants ou fournisseurs dans leurs installations respectives.

Article 11-1

Modifié par Loi n°2004-669 du 9 juillet 2004 art. 125 (JORF 10 juillet 2004).

Les personnes physiques ou morales qui fournissent des prestations de cryptologie visant à assurer une fonction de confidentialité sont tenues de remettre aux agents autorisés dans les conditions prévues à l'article 4, sur leur demande, les conventions permettant le déchiffrement des données transformées au moyen des prestations qu'elles ont fournies. Les agents autorisés peuvent demander aux fournisseurs de prestations susmentionnés de mettre eux-mêmes en oeuvre ces conventions, sauf si ceux-ci démontrent qu'ils ne sont pas en mesure de satisfaire à ces réquisitions.

Le fait de ne pas déférer, dans ces conditions, aux demandes des autorités habilitées est puni de deux ans d'emprisonnement et de 30000 euros d'amende.

Un décret en Conseil d'Etat précise les procédures suivant lesquelles cette obligation est mise en oeuvre ainsi que les conditions dans lesquelles la prise en charge financière de cette mise en oeuvre est assurée par l'Etat.

Article 12

Modifié par Loi n°2004-669 du 9 juillet 2004 art. 125 (JORF 10 juillet 2004).

Les transcriptions d'interceptions doivent être détruites dès que leur conservation n'est plus indispensable à la réalisation des fins mentionnées à l'article 3.

Il est dressé procès-verbal de l'opération de destruction.

Les opérations mentionnées aux alinéas précédents sont effectuées sous l'autorité du Premier ministre.

Article 13

Modifié par Loi n°2004-669 du 9 juillet 2004 art. 125 (JORF 10 juillet 2004).

Il est institué une Commission nationale de contrôle des interceptions de sécurité. Cette commission est une autorité administrative indépendante. Elle est chargée de veiller au respect des dispositions du présent titre. Elle est présidée par une personnalité désignée, pour une durée de six ans, par le Président de la République, sur une liste de quatre noms établie conjointement par le vice-président du Conseil d'Etat et le premier président de la Cour de cassation.

Elle comprend, en outre :

Un député désigné pour la durée de la législature par le président de l'Assemblée nationale ;

Un sénateur désigné après chaque renouvellement partiel du Sénat par le président du Sénat.

La qualité de membre de la commission est incompatible avec celle de membre du Gouvernement.

Sauf démission, il ne peut être mis fin aux fonctions de membre de la commission qu'en cas d'empêchement constaté par celle-ci.

Le mandat des membres de la commission n'est pas renouvelable.

En cas de partage des voix, la voix du président est prépondérante.

Les agents de la commission sont nommés par le président.

Les membres de la commission désignés en remplacement de ceux dont les fonctions ont pris fin avant leur terme normal achèvent le mandat de ceux qu'ils remplacent. A l'expiration de ce

mandat, par dérogation au septième alinéa ci-dessus, ils peuvent être nommés comme membre de la commission s'ils ont occupé ces fonctions de remplacement pendant moins de deux ans.

Les membres de la commission sont astreints au respect des secrets protégés par les articles 413-10, 226-13 et 226-14 du code pénal pour les faits, actes ou renseignements dont ils ont pu avoir connaissance en raison de leurs fonctions.

La commission établit son règlement intérieur.

Article 14

Modifié par Loi n°2004-669 du 9 juillet 2004 art. 125 (JORF 10 juillet 2004).

La décision motivée du Premier ministre mentionnée à l'article 4 est communiquée dans un délai de quarante-huit heures au plus tard au président de la Commission nationale de contrôle des interceptions de sécurité.

Si celui-ci estime que la légalité de cette décision au regard des dispositions du présent titre n'est pas certaine, il réunit la commission, qui statue dans les sept jours suivant la réception par son président de la communication mentionnée au premier alinéa.

Au cas où la commission estime qu'une interception de sécurité a été autorisée en méconnaissance des dispositions du présent titre, elle adresse au Premier ministre une recommandation tendant à ce que cette interception soit interrompue.

Elle porte également cette recommandation à la connaissance du ministre ayant proposé l'interception et du ministre chargé des communications électroniques.

La commission peut adresser au Premier ministre une recommandation relative au contingent et à sa répartition visés à l'article 5.

Le Premier ministre informe sans délai la commission des suites données à ses recommandations.

Article 15

Modifié par Loi n°2004-669 du 9 juillet 2004 art. 125 (JORF 10 juillet 2004).

De sa propre initiative ou sur réclamation de toute personne y ayant un intérêt direct et personnel, la commission peut procéder au contrôle de toute interception de sécurité en vue de vérifier si elle est effectuée dans le respect des dispositions du présent titre.

Si la commission estime qu'une interception de sécurité est effectuée en violation des dispositions du présent titre, elle adresse au Premier ministre une recommandation tendant à ce que cette interception soit interrompue.

Il est alors procédé ainsi qu'il est indiqué aux quatrième et sixième alinéas de l'article 14.

Article 16

Modifié par Loi n°2004-669 du 9 juillet 2004 art. 125 (JORF 10 juillet 2004).

Les ministres, les autorités publiques, les agents publics doivent prendre toutes mesures utiles pour faciliter l'action de la commission.

Article 17

Modifié par Loi n°2004-669 du 9 juillet 2004 art. 125 (JORF 10 juillet 2004).

Lorsque la commission a exercé son contrôle à la suite d'une réclamation, il est notifié à l'auteur de la réclamation qu'il a été procédé aux vérifications nécessaires.

Conformément au deuxième alinéa de l'article 40 du code de procédure pénale, la commission donne avis sans délai au procureur de la République de toute infraction aux dispositions de la présente loi dont elle a pu avoir connaissance à l'occasion du contrôle effectué en application de l'article 15.

Article 18

Modifié par Loi n°2005-1719 du 30 décembre 2005 art. 135 VI Finances pour 2006 (JORF 31 décembre 2005).

Les crédits nécessaires à la Commission nationale de contrôle des interceptions de sécurité pour l'accomplissement de sa mission sont inscrits au programme intitulé "Coordination du travail gouvernemental".

Le président est ordonnateur des dépenses de la commission.

Article 19

Modifié par Loi n°2006-64 du 23 janvier 2006 art. 6 III (JORF 24 janvier 2006).

La commission remet chaque année au Premier ministre un rapport sur les conditions d'exercice et les résultats de son activité, qui précise notamment le nombre de recommandations

qu'elle a adressées au Premier ministre en application de l'article 14 de la présente loi (1) et au ministre de l'intérieur en application de l'article L. 34-1-1 du code des postes et des communications électroniques et de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, ainsi que les suites qui leur ont été données. Ce rapport est rendu public.

Elle adresse, à tout moment, au Premier ministre les observations qu'elle juge utiles.

[. . .]

GERMANIA

Legge fondamentale

Art. 10

(1) Il segreto della corrispondenza e il segreto postale e delle telecomunicazioni sono inviolabili.

(2) Limitazioni possono essere poste solo con legge. Se la limitazione serve alla difesa dell'ordinamento costituzionale liberale e democratico o dell'esistenza o della sicurezza della Federazione o di un Land, la legge può stabilire che la misura restrittiva non venga comunicata all'interessato e che il ricorso giurisdizionale sia sostituito dal controllo di organi anche ausiliari, istituiti dal Parlamento.

Strafprozessordnung

(…)

Achter Abschnitt

Beschlagnahme, Überwachung des Fernmeldeverkehrs, Rasterfahndung, Einsatz technischer Mittel, Einsatz Verdeckter Ermittler und Durchsuchung

§ 100a

(1) Auch ohne Wissen der Betroffenen darf die Telekommunikation überwacht und aufgezeichnet werden, wenn

1. bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine in Absatz 2 bezeichnete schwere Straftat begangen, in Fällen, in denen der Versuch strafbar ist, zu begehen versucht, oder durch eine Straftat vorbereitet hat,
2. die Tat auch im Einzelfall schwer wiegt und
3. die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos wäre.

(2) Schwere Straftaten im Sinne des Absatzes 1 Nr. 1 sind:

1. aus dem Strafgesetzbuch:
   a) Straftaten des Friedensverrats, des Hochverrats und der Gefährdung des demokratischen Rechtsstaates sowie des Landesverrats und der Gefährdung der äußeren Sicherheit nach den §§ 80 bis 82, 84 bis 86, 87 bis 89, 94 bis 100a,
   b) Abgeordnetenbestechung nach § 108e,
   c) Straftaten gegen die Landesverteidigung nach den §§ 109d bis 109h,
   d) Straftaten gegen die öffentliche Ordnung nach den §§ 129 bis 130,
   e) Geld- und Wertzeichenfälschung nach den §§ 146 und 151, jeweils auch in Verbindung mit § 152, sowie nach § 152a Abs. 3 und § 152b Abs. 1 bis 4,
   f) Straftaten gegen die sexuelle Selbstbestimmung in den Fällen der §§ 176a, 176b, 177 Abs. 2 Nr. 2 und des § 179 Abs. 5 Nr. 2,
   g) Verbreitung, Erwerb und Besitz kinderpornografischer Schriften nach § 184b Abs. 1 bis 3,
   h) Mord und Totschlag nach den §§ 211 und 212,
   i) Straftaten gegen die persönliche Freiheit nach den §§ 232 bis 233a, 234, 234a, 239a und 239b,
   j) Bandendiebstahl nach § 244 Abs. 1 Nr. 2 und schwerer Bandendiebstahl nach § 244a,
   k) Straftaten des Raubes und der Erpressung nach den §§ 249 bis 255,
   l) gewerbsmäßige Hehlerei, Bandenhehlerei und gewerbsmäßige Bandenhehlerei nach den §§ 260 und 260a,
   m) Geldwäsche und Verschleierung unrechtmäßig erlangter Vermögenswerte nach § 261 Abs. 1, 2 und 4,
   n) Betrug und Computerbetrug unter den in § 263 Abs. 3 Satz 2 genannten Voraussetzungen und im Falle des § 263 Abs. 5, jeweils auch in Verbindung mit § 263a Abs. 2,
   o) Subventionsbetrug unter den in § 264 Abs. 2 Satz 2 genannten Voraussetzungen und im Falle des § 264 Abs. 3 in Verbindung mit § 263 Abs. 5,
   p) Straftaten der Urkundenfälschung unter den in § 267 Abs. 3 Satz 2 genannten Voraussetzungen und im Fall des § 267 Abs. 4, jeweils auch in Verbindung mit § 268 Abs. 5 oder § 269 Abs. 3, sowie nach § 275 Abs. 2 und § 276 Abs. 2,
   q) Bankrott unter den in § 283a Satz 2 genannten Voraussetzungen,

r) Straftaten gegen den Wettbewerb nach § 298 und, unter den in § 300 Satz 2 genannten Voraussetzungen, nach § 299,

s) gemeingefährliche Straftaten in den Fällen der §§ 306 bis 306c, 307 Abs. 1 bis 3, des § 308 Abs. 1 bis 3, des § 309 Abs. 1 bis 4, des § 310 Abs. 1, der §§ 313, 314, 315 Abs. 3, des § 315b Abs. 3 sowie der §§ 316a und 316c,

t) Bestechlichkeit und Bestechung nach den §§ 332 und 334,

2. aus der Abgabenordnung:

a) Steuerhinterziehung unter den in § 370 Abs. 3 Satz 2 Nr. 5 genannten Voraussetzungen,

b) gewerbsmäßiger, gewaltsamer und bandenmäßiger Schmuggel nach § 373,

c) Steuerhehlerei im Falle des § 374 Abs. 2,

3. aus dem Arzneimittelgesetz:

Straftaten nach § 95 Abs. 1 Nr. 2a unter den in § 95 Abs. 3 Satz 2 Nr. 2 Buchstabe b genannten Voraussetzungen,

4. aus dem Asylverfahrensgesetz:

a) Verleitung zur missbräuchlichen Asylantragstellung nach § 84 Abs. 3,

b) gewerbs- und bandenmäßige Verleitung zur missbräuchlichen Asylantragstellung nach § 84a,

5. aus dem Aufenthaltsgesetz:

a) Einschleusen von Ausländern nach § 96 Abs. 2,

b) Einschleusen mit Todesfolge und gewerbs- und bandenmäßiges Einschleusen nach § 97,

6. aus dem Außenwirtschaftsgesetz:

Straftaten nach § 34 Abs. 1 bis 6,

7. aus dem Betäubungsmittelgesetz:

a) Straftaten nach einer in § 29 Abs. 3 Satz 2 Nr. 1 in Bezug genommenen Vorschrift unter den dort genannten Voraussetzungen,

b) Straftaten nach den §§ 29a, 30 Abs. 1 Nr. 1, 2 und 4 sowie den §§ 30a und 30b,

8. aus dem Grundstoffüberwachungsgesetz:

Straftaten nach § 19 Abs. 1 unter den in § 19 Abs. 3 Satz 2 genannten Voraussetzungen,

9. aus dem Gesetz über die Kontrolle von Kriegswaffen:

a) Straftaten nach § 19 Abs. 1 bis 3 und § 20 Abs. 1 und 2 sowie § 20a Abs. 1 bis 3, jeweils auch in Verbindung mit § 21,

b) Straftaten nach § 22a Abs. 1 bis 3,

10. aus dem Völkerstrafgesetzbuch:

a) Völkermord nach § 6,

b) Verbrechen gegen die Menschlichkeit nach § 7,

c) Kriegsverbrechen nach den §§ 8 bis 12,

11. aus dem Waffengesetz:

a) Straftaten nach § 51 Abs. 1 bis 3,

b) Straftaten nach § 52 Abs. 1 Nr. 1 und 2 Buchstabe c und d sowie Abs. 5 und 6.

(3) Die Anordnung darf sich nur gegen den Beschuldigten oder gegen Personen richten, von denen auf Grund bestimmter Tatsachen anzunehmen ist, dass sie für den Beschuldigten bestimmte oder von ihm herrührende Mitteilungen entgegennehmen oder weitergeben oder dass der Beschuldigte ihren Anschluss benutzt.

(4) Liegen tatsächliche Anhaltspunkte für die Annahme vor, dass durch eine Maßnahme nach Absatz 1 allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt würden, ist die Maßnahme unzulässig. Erkenntnisse aus dem Kernbereich privater Lebensgestaltung, die durch eine Maßnahme nach Absatz 1 erlangt wurden, dürfen nicht verwertet werden.

Aufzeichnungen hierüber sind unverzüglich zu löschen. 4Die Tatsache ihrer Erlangung und Löschung ist aktenkundig zu machen.

§ 100b

(1) Maßnahmen nach §100a dürfen nur auf Antrag der Staatsanwaltschaft durch das Gericht angeordnet werden. Bei Gefahr im Verzug kann die Anordnung auch durch die Staatsanwaltschaft getroffen werden. Soweit die Anordnung der Staatsanwaltschaft nicht binnen drei Werktagen von dem Gericht bestätigt wird, tritt sie außer Kraft. Die Anordnung ist auf höchstens drei Monate zu befristen. Eine Verlängerung um jeweils nicht mehr als drei Monate ist zulässig, soweit die Voraussetzungen der Anordnung unter Berücksichtigung der gewonnenen Ermittlungsergebnisse fortbestehen.

(2) Die Anordnung ergeht schriftlich. 2In ihrer Entscheidungsformel sind anzugeben:

1. soweit möglich, der Name und die Anschrift des Betroffenen, gegen den sich die Maßnahme richtet,
2. die Rufnummer oder eine andere Kennung des zu überwachenden Anschlusses oder des Endgerätes, sofern sich nicht aus bestimmten Tatsachen ergibt, dass diese zugleich einem anderen Endgerät zugeordnet ist,
3. Art, Umfang und Dauer der Maßnahme unter Benennung des Endzeitpunktes.

(3) Auf Grund der Anordnung hat jeder, der Telekommunikationsdienste erbringt oder daran mitwirkt, dem Gericht, der Staatsanwaltschaft und ihren im Polizeidienst tätigen Ermittlungspersonen (§ 152 des Gerichtsverfassungsgesetzes) die Maßnahmen nach § 100a zu ermöglichen und die erforderlichen Auskünfte unverzüglich zu erteilen. 2Ob und in welchem Umfang hierfür Vorkehrungen zu treffen sind, bestimmt sich nach dem Telekommunikationsgesetz und der Telekommunikations-Überwachungsverordnung. 3§ 95 Abs. 2 gilt entsprechend.

(4) Liegen die Voraussetzungen der Anordnung nicht mehr vor, so sind die auf Grund der Anordnung ergriffenen Maßnahmen unverzüglich zu beenden. 2Nach Beendigung der Maßnahme ist das anordnende Gericht über deren Ergebnisse zu unterrichten.

(5) Die Länder und der Generalbundesanwalt berichten dem Bundesamt für Justiz kalenderjährlich jeweils bis zum 30. Juni des dem Berichtsjahr folgenden Jahres über in ihrem Zuständigkeitsbereich angeordnete Maßnahmen nach § 100a. 2Das Bundesamt für Justiz erstellt eine Übersicht zu den im Berichtsjahr bundesweit angeordneten Maßnahmen und veröffentlicht diese im Internet. 31)

(6) In den Berichten nach Absatz 5 sind anzugeben:

1. die Anzahl der Verfahren, in denen Maßnahmen nach § 100a Abs. 1 angeordnet worden sind;
2. die Anzahl der Überwachungsanordnungen nach § 100a Abs. 1, unterschieden nach
    a) Erst- und Verlängerungsanordnungen sowie
    b) Festnetz-, Mobilfunk- und Internettelekommunikation;
3. die jeweils zugrunde liegende Anlassstraftat nach Maßgabe der Unterteilung in § 100a Abs. 2.

Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz - G 10)

"Artikel 10-Gesetz vom 26. Juni 2001 (BGBl. I S. 1254, 2298), zuletzt geändert durch Artikel 5 des Gesetzes vom 21. Dezember 2007 (BGBl. I S. 3198)"

(…)

Abschnitt 2
Beschränkungen in Einzelfällen

§ 3 Voraussetzungen

(1) Beschränkungen nach § 1 Abs. 1 Nr. 1 dürfen unter den dort bezeichneten Voraussetzungen angeordnet werden, wenn tatsächliche Anhaltspunkte für den Verdacht bestehen, dass jemand

1. Straftaten des Friedensverrats oder des Hochverrats (§§ 80 bis 83 des Strafgesetzbuches),

2. Straftaten der Gefährdung des demokratischen Rechtsstaates (§§ 84 bis 86, 87 bis 89 des Strafgesetzbuches, § 20 Abs. 1 Nr. 1 bis 4 des Vereinsgesetzes),

3. Straftaten des Landesverrats und der Gefährdung der äußeren Sicherheit (§§ 94 bis 96, 97a bis 100a des Strafgesetzbuches),

4. Straftaten gegen die Landesverteidigung (§§ 109e bis 109g des Strafgesetzbuches),

5. Straftaten gegen die Sicherheit der in der Bundesrepublik Deutschland stationierten Truppen der nichtdeutschen Vertragsstaaten des Nordatlantikvertrages (§§ 87, 89, 94 bis 96, 98 bis 100, 109e bis 109g des Strafgesetzbuches in Verbindung mit § 1 des NATO-Truppen-Schutzgesetzes),

6. Straftaten nach

a) den §§ 129a bis 130 des Strafgesetzbuches sowie

b) den §§ 211, 212, 239a, 239b, 306 bis 306c, 308 Abs. 1 bis 3, § 315 Abs. 3, § 316b Abs. 3 und § 316c Abs. 1 und 3 des Strafgesetzbuches, soweit diese sich gegen die freiheitliche demokratische Grundordnung, den Bestand oder die Sicherheit des Bundes oder eines Landes richten, oder

7. Straftaten nach § 95 Abs. 1 Nr. 8 des Aufenthaltsgesetzes

plant, begeht oder begangen hat. 2Gleiches gilt, wenn tatsächliche Anhaltspunkte für den Verdacht bestehen, dass jemand Mitglied einer Vereinigung ist, deren Zwecke oder deren Tätigkeit darauf gerichtet sind, Straftaten zu begehen, die gegen die freiheitliche demokratische Grundordnung, den Bestand oder die Sicherheit des Bundes oder eines Landes gerichtet sind.

(2) Die Anordnung ist nur zulässig, wenn die Erforschung des Sachverhalts auf andere Weise aussichtslos oder wesentlich erschwert wäre. Sie darf sich nur gegen den Verdächtigen oder gegen Personen richten, von denen auf Grund bestimmter Tatsachen anzunehmen ist, dass sie für den Verdächtigen bestimmte oder von ihm herrührende Mitteilungen entgegennehmen oder weitergeben oder dass der Verdächtige ihren Anschluss benutzt. Maßnahmen, die sich auf Sendungen beziehen, sind nur hinsichtlich solcher Sendungen zulässig, bei denen Tatsachen die Annahme rechtfertigen, dass sie von dem, gegen den sich die Anordnung richtet, herrühren oder für ihn bestimmt sind. Abgeordnetenpost von Mitgliedern des Deutschen Bundestages und der

Parlamente der Länder darf nicht in eine Maßnahme einbezogen werden, die sich gegen einen Dritten richtet.

§ 4 Prüf-, Kennzeichnungs- und Löschungspflichten, Übermittlungen, Zweckbindung

(1) Die erhebende Stelle prüft unverzüglich und sodann in Abständen von höchstens sechs Monaten, ob die erhobenen personenbezogenen Daten im Rahmen ihrer Aufgaben allein oder zusammen mit bereits vorliegenden Daten für die in § 1 Abs. 1 Nr. 1 bestimmten Zwecke erforderlich sind. Soweit die Daten für diese Zwecke nicht erforderlich sind und nicht für eine Übermittlung an andere Stellen benötigt werden, sind sie unverzüglich unter Aufsicht eines Bediensteten, der die Befähigung zum Richteramt hat, zu löschen. Die Löschung ist zu protokollieren. Sie unterbleibt, soweit die Daten für eine Mitteilung nach §12 Abs. 1 oder für eine gerichtliche Nachprüfung der Rechtmäßigkeit der Beschränkungsmaßnahme von Bedeutung sein können. In diesem Fall sind die Daten zu sperren; sie dürfen nur zu diesen Zwecken verwendet werden.

(2) Die verbleibenden Daten sind zu kennzeichnen. Nach einer Übermittlung ist die Kennzeichnung durch den Empfänger aufrechtzuerhalten. Die Daten dürfen nur zu den in § 1 Abs. 1 Nr. 1 und den in Absatz 4 genannten Zwecken verwendet werden.

(3) Der Behördenleiter oder sein Stellvertreter kann anordnen, dass bei der Übermittlung auf die Kennzeichnung verzichtet wird, wenn dies unerlässlich ist, um die Geheimhaltung einer Beschränkungsmaßnahme nicht zu gefährden, und die G 10-Kommission oder, soweit es sich um die Übermittlung durch eine Landesbehörde handelt, die nach Landesrecht zuständige Stelle zugestimmt hat. Bei Gefahr im Verzuge kann die Anordnung bereits vor der Zustimmung getroffen werden. Wird die Zustimmung versagt, ist die Kennzeichnung durch den Übermittlungsempfänger unverzüglich nachzuholen; die übermittelnde Behörde hat ihn hiervon zu unterrichten.

(4) Die Daten dürfen nur übermittelt werden

1. zur Verhinderung oder Aufklärung von Straftaten, wenn

a) tatsächliche Anhaltspunkte für den Verdacht bestehen, dass jemand eine der in § 3 Abs. 1 genannten Straftaten plant oder begeht,

b) bestimmte Tatsachen den Verdacht begründen, dass jemand eine sonstige in § 7 Abs. 4 Satz 1 genannte Straftat plant oder begeht,

2. zur Verfolgung von Straftaten, wenn bestimmte Tatsachen den Verdacht begründen, dass jemand eine in Nummer 1 bezeichnete Straftat begeht oder begangen hat, oder

3. zur Vorbereitung und Durchführung eines Verfahrens nach Artikel 21 Abs. 2 Satz 2 des Grundgesetzes oder einer Maßnahme nach § 3 Abs. 1 Satz 1 des Vereinsgesetzes,

soweit sie zur Erfüllung der Aufgaben des Empfängers erforderlich sind.

(5) Sind mit personenbezogenen Daten, die übermittelt werden dürfen, weitere Daten des Betroffenen oder eines Dritten in Akten so verbunden, dass eine Trennung nicht oder nur mit unvertretbarem Aufwand möglich ist, ist die Übermittlung auch dieser Daten zulässig; eine Verwendung dieser Daten ist unzulässig. 2Über die Übermittlung entscheidet ein Bediensteter der übermittelnden Stelle, der die Befähigung zum Richteramt hat. 3Die Übermittlung ist zu protokollieren.

(6) Der Empfänger darf die übermittelten Daten nur für die Zwecke verwenden, zu deren Erfüllung sie ihm übermittelt worden sind. Er prüft unverzüglich und sodann in Abständen von höchstens sechs Monaten, ob die übermittelten Daten für diese Zwecke erforderlich sind. Absatz 1

Satz 2 und 3 gilt entsprechend. Der Empfänger unterrichtet die übermittelnde Stelle unverzüglich über die erfolgte Löschung.

Abschnitt 3
Strategische Beschränkungen

§ 5 Voraussetzungen

(1) Auf Antrag des Bundesnachrichtendienstes dürfen Beschränkungen nach § 1 für internationale Telekommunikationsbeziehungen, soweit eine gebündelte Übertragung erfolgt, angeordnet werden. Die jeweiligen Telekommunikationsbeziehungen werden von dem nach § 10 Abs. 1 zuständigen Bundesministerium mit Zustimmung des Parlamentarischen Kontrollgremiums bestimmt. Beschränkungen nach Satz 1 sind nur zulässig zur Sammlung von Informationen über Sachverhalte, deren Kenntnis notwendig ist, um die Gefahr

1. eines bewaffneten Angriffs auf die Bundesrepublik Deutschland,

2. der Begehung internationaler terroristischer Anschläge mit unmittelbarem Bezug zur Bundesrepublik Deutschland,

3. der internationalen Verbreitung von Kriegswaffen im Sinne des Gesetzes über die Kontrolle von Kriegswaffen sowie des unerlaubten Außenwirtschaftsverkehrs mit Waren, Datenverarbeitungsprogrammen und Technologien in Fällen von erheblicher Bedeutung,

4. der unbefugten Verbringung von Betäubungsmitteln in nicht geringer Menge in die Bundesrepublik Deutschland,

5. der Beeinträchtigung der Geldwertstabilität im Euro-Währungsraum durch im Ausland begangene Geldfälschungen oder

6. der international organisierten Geldwäsche in Fällen von erheblicher Bedeutung

rechtzeitig zu erkennen und einer solchen Gefahr zu begegnen. 4In den Fällen von Satz 3 Nr. 1 dürfen Beschränkungen auch für Postverkehrsbeziehungen angeordnet werden; Satz 2 gilt entsprechend.

(2) Bei Beschränkungen von Telekommunikationsbeziehungen darf der Bundesnachrichtendienst nur Suchbegriffe verwenden, die zur Aufklärung von Sachverhalten über den in der Anordnung bezeichneten Gefahrenbereich bestimmt und geeignet sind. Die Suchbegriffe dürfen keine Identifizierungsmerkmale enthalten, die zu einer gezielten Erfassung bestimmter Telekommunikationsanschlüsse führen. Dies gilt nicht für Telekommunikationsanschlüsse im Ausland, sofern ausgeschlossen werden kann, dass Anschlüsse, deren Inhaber oder regelmäßige Nutzer deutsche Staatsangehörige sind, gezielt erfasst werden. Die Durchführung ist zu protokollieren. Die Protokolldaten dürfen ausschließlich zu Zwecken der Datenschutzkontrolle verwendet werden. Sie sind am Ende des Kalenderjahres, das dem Jahr der Protokollierung folgt, zu löschen.

§ 6 Prüf-, Kennzeichnungs- und Löschungspflichten, Zweckbindung

(1) Der Bundesnachrichtendienst prüft unverzüglich und sodann in Abständen von höchstens sechs Monaten, ob die erhobenen personenbezogenen Daten im Rahmen seiner Aufgaben allein

oder zusammen mit bereits vorliegenden Daten für die in § 5 Abs. 1 Satz 3 bestimmten Zwecke erforderlich sind. Soweit die Daten für diese Zwecke nicht erforderlich sind und nicht für eine Übermittlung an andere Stellen benötigt werden, sind sie unverzüglich unter Aufsicht eines Bediensteten, der die Befähigung zum Richteramt hat, zu löschen. Die Löschung ist zu protokollieren. Außer in den Fällen der erstmaligen Prüfung nach Satz 1 unterbleibt die Löschung, soweit die Daten für eine Mitteilung nach § 12 Abs. 2 oder für eine gerichtliche Nachprüfung der Rechtmäßigkeit der Beschränkungsmaßnahme von Bedeutung sein können. In diesem Fall sind die Daten zu sperren; sie dürfen nur zu diesen Zwecken verwendet werden.

(2) Die verbleibenden Daten sind zu kennzeichnen. Nach einer Übermittlung ist die Kennzeichnung durch den Empfänger aufrechtzuerhalten. Die Daten dürfen nur zu den in § 5 Abs. 1 Satz 3 genannten Zwecken und für Übermittlungen nach § 7 Abs. 1 bis 4 verwendet werden.

§ 7 Übermittlungen durch den Bundesnachrichtendienst

(1) Durch Beschränkungen nach § 5 erhobene personenbezogene Daten dürfen nach § 12 des BND-Gesetzes zur Unterrichtung über die in § 5 Abs. 1 Satz 3 genannten Gefahren übermittelt werden.

(2) Durch Beschränkungen nach § 5 erhobene personenbezogene Daten dürfen an die Verfassungsschutzbehörden des Bundes und der Länder sowie an den Militärischen Abschirmdienst übermittelt werden, wenn

1. tatsächliche Anhaltspunkte dafür bestehen, dass die Daten erforderlich sind zur Sammlung und Auswertung von Informationen über Bestrebungen in der Bundesrepublik Deutschland, die durch Anwendung von Gewalt oder darauf gerichtete Vorbereitungshandlungen gegen die in § 3 Abs. 1 Nr. 1, 3 und 4 des Bundesverfassungsschutzgesetzes genannten Schutzgüter gerichtet sind, oder

2. bestimmte Tatsachen den Verdacht sicherheitsgefährdender oder geheimdienstlicher Tätigkeiten für eine fremde Macht begründen.

(3) Durch Beschränkungen nach § 5 Abs. 1 Satz 1 in Verbindung mit Satz 3 Nr. 3 erhobene personenbezogene Daten dürfen an das Bundesamt für Wirtschaft und Ausfuhrkontrolle (BAFA) übermittelt werden, wenn tatsächliche Anhaltspunkte dafür bestehen, dass die Kenntnis dieser Daten erforderlich ist

1. zur Aufklärung von Teilnehmern am Außenwirtschaftsverkehr über Umstände, die für die Einhaltung von Beschränkungen des Außenwirtschaftsverkehrs von Bedeutung sind, oder

2. im Rahmen eines Verfahrens zur Erteilung einer ausfuhrrechtlichen Genehmigung oder zur Unterrichtung von Teilnehmern am Außenwirtschaftsverkehr, soweit hierdurch eine Genehmigungspflicht für die Ausfuhr von Gütern begründet wird.

(4) Durch Beschränkungen nach § 5 erhobene personenbezogene Daten dürfen zur Verhinderung von Straftaten an die mit polizeilichen Aufgaben betrauten Behörden übermittelt werden, wenn

1. tatsächliche Anhaltspunkte für den Verdacht bestehen, dass jemand

a) Straftaten nach § 129a, auch in Verbindung mit § 129b Abs. 1, sowie den §§ 146, 151 bis 152a oder § 261 des Strafgesetzbuches,

b) Straftaten nach § 34 Abs. 1 bis 6 und 8, § 35 des Außenwirtschaftsgesetzes, §§ 19 bis 21 oder § 22a Abs. 1 Nr. 4, 5 und 7 des Gesetzes über die Kontrolle von Kriegswaffen oder

c) Straftaten nach § 29a Abs. 1 Nr. 2, § 30 Abs. 1 Nr. 1, 4 oder § 30a des Betäubungsmittelgesetzes

plant oder begeht oder

2. bestimmte Tatsachen den Verdacht begründen, dass jemand

a) Straftaten, die in § 3 Abs. 1 Satz 1 Nr. 1 bis 5 und 7, Satz 2 dieses Gesetzes oder in § 129a Abs. 1 des Strafgesetzbuches bezeichnet sind, oder

b) Straftaten nach den §§ 130, 232 Abs. 3, 4 oder Abs. 5 zweiter Halbsatz, §§ 249 bis 251, 255, 305a, 306 bis 306c, 307 Abs. 1 bis 3, § 308 Abs. 1 bis 4, § 309 Abs. 1 bis 5, §§ 313, 314, 315 Abs. 1, 3 oder Abs. 4, § 315b Abs. 3, §§ 316a, 316b Abs. 1 oder Abs. 3 oder § 316c Abs. 1 bis 3 des Strafgesetzbuches

plant oder begeht. Die Daten dürfen zur Verfolgung von Straftaten an die zuständigen Behörden übermittelt werden, wenn bestimmte Tatsachen den Verdacht begründen, dass jemand eine in Satz 1 bezeichnete Straftat begeht oder begangen hat.

(5) Die Übermittlung ist nur zulässig, soweit sie zur Erfüllung der Aufgaben des Empfängers erforderlich ist. Sind mit personenbezogenen Daten, die übermittelt werden dürfen, weitere Daten des Betroffenen oder eines Dritten in Akten so verbunden, dass eine Trennung nicht oder nur mit unvertretbarem Aufwand möglich ist, ist die Übermittlung auch dieser Daten zulässig; eine Verwendung dieser Daten ist unzulässig. Über die Übermittlung entscheidet ein Bediensteter des Bundesnachrichtendienstes, der die Befähigung zum Richteramt hat. 4Die Übermittlung ist zu protokollieren.

(6) Der Empfänger darf die Daten nur für die Zwecke verwenden, zu deren Erfüllung sie ihm übermittelt worden sind. 2Er prüft unverzüglich und sodann in Abständen von höchstens sechs Monaten, ob die übermittelten Daten für diese Zwecke erforderlich sind. 3§ 6 Abs. 1 Satz 2 und 3 gilt entsprechend.

§ 8 Gefahr für Leib oder Leben einer Person im Ausland

(1) Auf Antrag des Bundesnachrichtendienstes dürfen Beschränkungen nach § 1 für internationale Telekommunikationsbeziehungen im Sinne des § 5 Abs. 1 Satz 1 angeordnet werden, wenn dies erforderlich ist, um eine im Einzelfall bestehende Gefahr für Leib oder Leben einer Person im Ausland rechtzeitig zu erkennen oder ihr zu begegnen und dadurch Belange der Bundesrepublik Deutschland unmittelbar in besonderer Weise berührt sind. 2§ 5 Abs. 1 Satz 2 gilt entsprechend.

(2) Die Zustimmung des Parlamentarischen Kontrollgremiums bedarf der Mehrheit von zwei Dritteln seiner Mitglieder. Die Bestimmung tritt spätestens nach zwei Monaten außer Kraft. Eine erneute Bestimmung ist zulässig, soweit ihre Voraussetzungen fortbestehen.

(3) Die Anordnung ist nur zulässig, wenn die Erforschung des Sachverhalts auf andere Weise aussichtslos oder wesentlich erschwert wäre. Der Bundesnachrichtendienst darf nur Suchbegriffe verwenden, die zur Erlangung von Informationen über die in der Anordnung bezeichnete Gefahr bestimmt und geeignet sind. 3§ 5 Abs. 2 Satz 2 bis 6 gilt entsprechend.

(4) Der Bundesnachrichtendienst prüft unverzüglich und sodann in Abständen von höchstens sechs Monaten, ob die erhobenen personenbezogenen Daten im Rahmen seiner Aufgaben allein oder zusammen mit bereits vorliegenden Daten zu dem in Absatz 1 bestimmten Zweck erforderlich sind. Soweit die Daten für diesen Zweck nicht erforderlich sind, sind sie unverzüglich unter Aufsicht

eines Bediensteten, der die Befähigung zum Richteramt hat, zu löschen. Die Löschung ist zu protokollieren. §6 Abs. 1 Satz 4 und 5, Abs. 2 Satz 1 und 2 gilt entsprechend. Die Daten dürfen nur zu den in den Absätzen 1, 5 und 6 genannten Zwecken verwendet werden.

(5) Die erhobenen personenbezogenen Daten dürfen nach § 12 des BND-Gesetzes zur Unterrichtung über die in Absatz 1 genannte Gefahr übermittelt werden.

(6) Die erhobenen personenbezogenen Daten dürfen zur Verhinderung von Straftaten an die zuständigen Behörden übermittelt werden, wenn tatsächliche Anhaltspunkte den Verdacht begründen, dass jemand eine Straftat plant oder begeht, die geeignet ist, zu der Entstehung oder Aufrechterhaltung der in Absatz 1 bezeichneten Gefahr beizutragen. Die Daten dürfen zur Verfolgung von Straftaten an die zuständigen Behörden übermittelt werden, wenn bestimmte Tatsachen den Verdacht begründen, dass jemand eine in Satz 1 bezeichnete Straftat begeht oder begangen hat. §7 Abs. 5 und 6 gilt entsprechend.

Gesetz über das Zollkriminalamt und die Zollfahndungsämter

(Zollfahndungsdienstgesetz - ZFdG)

"Zollfahndungsdienstgesetz vom 16. August 2002 (BGBl. I S. 3202), zuletzt geändert durch Artikel 4 des Gesetzes vom 13. Dezember 2007 (BGBl. I S. 2897)"

(…)

Abschnitt 3
Präventive Telekommunikations- und Postüberwachung

§ 23a Beschränkung des Brief-, Post- und Fernmeldegeheimnisses

(1) Rechtfertigen Tatsachen die Annahme, dass Personen Straftaten nach § 19 Abs. 1 oder 2, § 20 Abs. 1, § 20a Abs. 1 oder 2 oder § 22a Abs. 1 Nr. 4, 5 und 7 oder Abs. 2 des Gesetzes über die Kontrolle von Kriegswaffen vorbereiten, ist das Zollkriminalamt befugt, zur Verhütung dieser Straftaten dem Brief- oder Postgeheimnis unterliegende Sendungen zu öffnen und einzusehen sowie die dem Fernmeldegeheimnis unterliegende Telekommunikation zu überwachen und aufzuzeichnen. Die Überwachung und Aufzeichnung bedarf der vorherigen richterlichen Anordnung.

(2) Eine Vorbereitung von Straftaten im Sinne von Absatz 1 Satz 1 ist eine Handlung, die darauf gerichtet ist, Straftaten zu begehen, das geschützte Rechtsgut aber nicht unmittelbar gefährdet. Insbesondere fallen darunter das Führen von Verhandlungen über die Lieferung von Gütern oder das Erbringen von Dienstleistungen, das Anbieten, der Erwerb, die Herstellung oder die Überlassung von Gütern, das Anbieten von Dienstleistungen, die Beschaffung von Transportmitteln für die Lieferung von Gütern oder das Anwerben von Teilnehmern, soweit dies der Begehung der Straftat nützlich sein soll.

(3) Die Absätze 1 und 2 gelten entsprechend, wenn Tatsachen die Annahme rechtfertigen, dass Personen die öffentliche Sicherheit und Ordnung erheblich gefährden, indem sie rechtswidrig und ohne die hierfür erforderliche Genehmigung oder Entscheidung nach Artikel 4 Abs. 4 in Verbindung mit Abs. 1 oder 2 der Verordnung (EG) Nr. 1334/2000 vom 22. Juni 2000 oder nach § 5c oder § 5d der Außenwirtschaftsverordnung die Ausfuhr von

1. Waffen, Munition und Rüstungsmaterial einschließlich darauf bezogener Herstellungsausrüstung und Technologie, sowie von Gütern, die geeignet sind und von denen auf Grund von Tatsachen angenommen werden kann, dass sie ganz oder teilweise für eine militärische Endbestimmung im Sinne von Artikel 4 Abs. 2 Satz 2 der Verordnung (EG) Nr. 1334/2000 vom 22. Juni 2000 oder im Sinne von § 5c der Außenwirtschaftsverordnung bestimmt sind,

   a) wenn diese für die Verwendung in einem Staat bestimmt sind, der sich in einem internationalen oder nicht internationalen bewaffneten Konflikt befindet oder in dem die dringende Gefahr eines solchen Konfliktes besteht, oder

   b) wenn gegen das Käufer- oder Bestimmungsland oder gegen den Empfänger der Güter ein Waffenembargo auf Grund eines vom Rat der Europäischen Union verabschiedeten Gemeinsamen Standpunktes oder einer verbindlichen Resolution des Sicherheitsrates der Vereinten Nationen verhängt wurde und die Länder oder die Rechtsakte der Europäischen Union oder des Sicherheitsrates der Vereinten Nationen, auf

Grund derer die Liste der Empfänger erstellt wurde, in einer Veröffentlichung des Bundesministeriums für Wirtschaft und Technologie im Bundesanzeiger benannt sind, oder

c) wenn das Käufer- oder Bestimmungsland ein Land der Länderliste K (Anlage zur Außenwirtschaftsverordnung) ist oder

d) wenn durch die Lieferung der Güter die Gefahr eines schweren Nachteils für die äußere Sicherheit der Bundesrepublik Deutschland herbeigeführt wird,

2. Gütern, die ganz oder teilweise geeignet sind und von denen auf Grund von Tatsachen angenommen werden kann, dass sie dazu bestimmt sind, einen erheblichen Beitrag zur Entwicklung, Herstellung, Wartung, Lagerung oder zum Einsatz von Atomwaffen, biologischen oder chemischen Waffen zu leisten, oder

3. Gütern, die ganz oder teilweise geeignet sind und von denen auf Grund von Tatsachen angenommen werden kann, dass sie dazu bestimmt sind, einen erheblichen Beitrag zur Entwicklung, Herstellung, Wartung, Lagerung oder zum Einsatz von Flugkörpern für Atomwaffen, biologischen oder chemischen Waffen zu leisten oder,

4. Gütern, die ganz oder teilweise geeignet sind und von denen auf Grund von Tatsachen angenommen werden kann, dass sie dazu bestimmt sind, einen erheblichen Beitrag zur Errichtung, zum Betrieb einer oder zum Einbau in eine Anlage für kerntechnische Zwecke im Sinne der Kategorie 0 des Teils I Abschnitt C der Ausfuhrliste (Anlage AL zur Außenwirtschaftsverordnung) zu leisten und das Käufer- oder Bestimmungsland Algerien, Indien, Irak, Iran, Israel, Jordanien, Libyen, Nordkorea, Pakistan oder Syrien ist,

vorbereiten.

(4) Beschränkungen nach Absatz 1 oder 3 dürfen auch angeordnet werden gegenüber einer natürlichen Person oder gegenüber einer juristischen Person oder Personenvereinigung, wenn

1. Personen, bei denen die Voraussetzungen für die Anordnung von Beschränkungen nach Absatz 1 oder 3 vorliegen, für sie tätig sind und Tatsachen die Annahme rechtfertigen, dass diese an ihrem Postverkehr teilnehmen oder ihren Telekommunikationsanschluss oder ihr Endgerät benutzen, oder

2. sie für Personen, bei denen die Voraussetzungen für die Anordnung von Beschränkungen nach Absatz 1 oder 3 vorliegen, Mitteilungen entgegennehmen oder von diesen herrührende Mitteilungen weitergeben oder

3. Personen, bei denen die Voraussetzungen für die Anordnung von Beschränkungen nach Absatz 1 oder 3 vorliegen, ihren Telekommunikationsanschluss oder ihr Endgerät benutzen.

Beschränkungen nach Satz 1 dürfen nur angeordnet werden, wenn die Erkenntnisse aus Maßnahmen gegen Personen, bei denen die Voraussetzungen nach Absatz 1 oder 3 vorliegen, nicht ausreichen werden, um die in Vorbereitung befindliche Tat zu verhüten.

(4a) Beschränkungen nach Absatz 1, 3 oder 4 sind unzulässig, wenn tatsächliche Anhaltspunkte für die Annahme vorliegen, dass durch sie allein Kommunikationsinhalte aus dem Kernbereich privater Lebensgestaltung erlangt würden. Kommunikationsinhalte aus dem Kernbereich privater Lebensgestaltung, die durch eine Beschränkung nach Absatz 1, 3 oder 4 erlangt worden sind, dürfen nicht verwertet werden. Sie sind unverzüglich unter Aufsicht eines Bediensteten, der die Befähigung zum Richteramt hat, zu löschen. Die Tatsache der Erfassung der Daten und ihrer Löschung ist zu dokumentieren. Diese Daten dürfen ausschließlich zu Zwecken der Datenschutzkontrolle verwendet werden. Sie sind zu löschen, wenn sie für diese Zwecke nicht mehr erforderlich sind, spätestens jedoch am Ende des Kalenderjahres, das dem Jahr der Dokumentierung folgt.

(5) Eine Maßnahme, die sich gegen eine in § 53 Abs. 1 Satz 1 Nr. 1, 2 oder Nr. 4, jeweils auch in Verbindung mit § 53a der Strafprozessordnung, genannte Person richtet und voraussichtlich Erkenntnisse erbringen würde, über die diese Person das Zeugnis verweigern dürfte, ist unzulässig. Dennoch erlangte Erkenntnisse dürfen nicht verwertet werden. Aufzeichnungen hierüber sind unverzüglich zu löschen. Die Tatsache ihrer Erlangung und der Löschung der Aufzeichnungen ist zu dokumentieren. Die Sätze 2 bis 4 gelten entsprechend, wenn durch eine

Maßnahme, die sich nicht gegen eine in § 53 Abs. 1 Satz 1 Nr. 1, 2 oder Nr. 4, jeweils auch in Verbindung mit § 53a der Strafprozessordnung, genannte Person richtet, von dieser Person Erkenntnisse erlangt werden, über die sie das Zeugnis verweigern dürfte. Soweit durch eine Maßnahme eine in § 53 Abs. 1 Satz 1 Nr. 3 bis 3b oder Nr. 5, jeweils auch in Verbindung mit § 53a der Strafprozessordnung, genannte Person betroffen wäre und dadurch voraussichtlich Erkenntnisse erlangt würden, über die diese Person das Zeugnis verweigern dürfte, ist dies im Rahmen der Prüfung der Verhältnismäßigkeit unter Würdigung des öffentlichen Interesses an den von dieser Person wahrgenommenen Aufgaben und des Interesses an der Geheimhaltung der dieser Person anvertrauten oder bekannt gewordenen Tatsachen besonders zu berücksichtigen. Soweit hiernach geboten, ist die Maßnahme zu unterlassen oder, soweit dies nach der Art der Maßnahme möglich ist, zu beschränken.

(5a) Absatz 5 gilt nicht, wenn Tatsachen die Annahme rechtfertigen, dass die dort genannten Personen an der Vorbereitung einer Tat nach Absatz 1 oder 3 beteiligt sind. 2Die Verwendung von Daten im Sinne von Absatz 5 Satz 2 ist zur Abwehr einer im Einzelfall bestehenden Lebensgefahr oder einer dringenden Gefahr für Leib oder Freiheit einer Person zulässig.

(6) Beschränkungen nach Absatz 1, 3 oder 4 dürfen nur angeordnet werden, wenn es ohne die Erkenntnisse aus den damit verbundenen Maßnahmen aussichtslos oder wesentlich erschwert wäre, die vorbereiteten Taten zu verhindern und die Maßnahmen nicht außer Verhältnis zur Schwere der zu verhindernden Tat stehen. Die Maßnahmen dürfen auch durchgeführt werden, wenn andere Personen unvermeidbar betroffen werden.

(7) Vor dem Antrag auf Anordnung nach § 23b ist die Staatsanwaltschaft zu unterrichten. Ebenso ist die Staatsanwaltschaft von der richterlichen Entscheidung, von einer Entscheidung des Bundesministeriums der Finanzen bei Gefahr im Verzug und von dem Ergebnis der durchgeführten Maßnahme zu unterrichten.

(8) § 2 des Artikel 10-Gesetzes gilt entsprechend.

§ 23b Gerichtliche Anordnung

(1) Die Anordnung nach § 23a Abs. 1, 3 oder 4 ergeht auf zu begründenden Antrag der Behördenleitung des Zollkriminalamts persönlich, bei deren Verhinderung von deren Stellvertretung, nach Zustimmung des Bundesministeriums der Finanzen durch das Landgericht. Bei Gefahr im Verzug kann die Anordnung vom Bundesministerium der Finanzen getroffen werden; sie tritt außer Kraft, wenn sie nicht binnen drei Tagen vom Landgericht bestätigt wird. Die gewonnenen Erkenntnisse dürfen nicht verwertet werden. Damit im Zusammenhang stehende Unterlagen sind unverzüglich zu vernichten.

(2) In der Begründung der Anordnung oder Verlängerung sind deren Voraussetzungen und die wesentlichen Abwägungsgesichtspunkte darzulegen. Insbesondere sind einzelfallbezogen anzugeben

1. die Bezeichnung der zu verhindernden Tat;
2. die Tatsachen, die die Annahme rechtfertigen, dass die Tat vorbereitet wird;
3. die wesentlichen Erwägungen zur Erforderlichkeit und Verhältnismäßigkeit der Maßnahme.

(3) Zuständig ist das Landgericht, in dessen Bezirk das Zollkriminalamt seinen Sitz hat. Das Landgericht entscheidet durch eine mit drei Richtern einschließlich des Vorsitzenden besetzte Kammer. Für das Verfahren gelten die Vorschriften des Gesetzes über die Angelegenheiten der freiwilligen Gerichtsbarkeit entsprechend.

(4) Die Anordnung ergeht schriftlich. Sie enthält

1. soweit bekannt den Namen und die Anschrift des Betroffenen, gegen den sie sich richtet,
2. bei einer Überwachung der Telekommunikation zusätzlich die Rufnummer oder eine andere Kennung des Telekommunikationsanschlusses oder die Kennung des Endgerätes, wenn diese allein diesem Endgerät zuzuordnen ist,

3. die Bestimmung von Art, Umfang und Dauer der Maßnahmen.

Die Anordnung ist auf höchstens drei Monate zu befristen. Auf Antrag der Behördenleitung des Zollkriminalamtes persönlich, bei deren Verhinderung von deren Stellvertretung, mit Zustimmung des Bundesministeriums der Finanzen, der unter Darstellung der bisherigen Ermittlungsergebnisse zu begründen ist, ist eine Verlängerung um jeweils bis zu drei Monaten zulässig, soweit die Voraussetzungen fortbestehen und eine weitere Überwachung verhältnismäßig ist. Wird eine Maßnahme nach § 23a Abs. 1, 3 oder 4 auf Grund einer Verlängerung die Dauer von neun Monaten überschreiten, so entscheidet das Oberlandesgericht über die weiteren Verlängerungen.

§ 23c Durchführungsvorschriften

(1) Die angeordnete Telekommunikations-, Brief- und Postüberwachung nach § 23a Abs. 1, 3 oder 4 ist durch das Zollkriminalamt vorzunehmen. Die Leitung der Maßnahme ist von einem Bediensteten mit der Befähigung zum Richteramt wahrzunehmen. 3§ 11 Abs. 2 und 3 des Artikel 10-Gesetzes ist entsprechend anzuwenden.

(2) Das Zollkriminalamt darf die durch die Maßnahmen erlangten personenbezogenen Daten zum Zwecke der Verhütung von Taten im Sinne des § 23a Abs. 1 oder 3 verarbeiten und nutzen. Es darf die Daten auch zur Verfolgung von Straftaten nach § 19 Abs. 1 bis 3, § 20 Abs. 1 oder 2, § 20a Abs. 1 bis 3, jeweils auch in Verbindung mit § 21, oder § 22a Abs. 1 bis 3 des Gesetzes über die Kontrolle von Kriegswaffen oder § 34 Abs. 1 bis 6 des Außenwirtschaftsgesetzes verwenden. Das Zollkriminalamt prüft unverzüglich und sodann in Abständen von höchstens sechs Monaten, ob die erhobenen Daten für die in § 23a Abs. 1 oder 3 bestimmten Zwecke erforderlich sind. 4Soweit die Daten für diese Zwecke nicht erforderlich sind, nicht zur Verfolgung einer Straftat im Sinne des Satzes 2 oder für eine Übermittlung nach § 23d benötigt werden sowie nicht mehr für eine Mitteilung nach Absatz 4 oder für eine gerichtliche Nachprüfung der Rechtmäßigkeit der Beschränkungsmaßnahme von Bedeutung sein können, sind sie unverzüglich unter Aufsicht eines Bediensteten, der die Befähigung zum Richteramt hat, zu löschen. Die Löschung ist zu protokollieren. Zur Sicherung der ordnungsgemäßen Löschung sind in regelmäßigen Abständen von höchstens sechs Monaten Prüfungen durch einen Bediensteten, der die Befähigung zum Richteramt hat, durchzuführen; die Prüfungen sind zu protokollieren. Daten, die nur zum Zwecke einer Mitteilung nach Absatz 4 oder der gerichtlichen Nachprüfung der Rechtmäßigkeit der Beschränkung gespeichert bleiben, sind zu sperren; sie dürfen nur zu diesem Zweck verwendet werden.

(3) Die erhobenen Daten sind zu kennzeichnen. Nach einer Übermittlung an die in § 23d Abs. 1 bis 7 bezeichneten Stellen ist die Kennzeichnung durch den Dritten, an den die Daten übermittelt wurden, aufrechtzuerhalten.

(4) Von den nach § 23a Abs. 1, 3, 4 oder 6 Satz 2 durchgeführten Maßnahmen hat das Zollkriminalamt die Betroffenen zu benachrichtigen. Dabei ist auf die Möglichkeit nachträglichen Rechtsschutzes nach Absatz 7 und die dafür vorgesehene Frist hinzuweisen. 3Betroffene im Sinne von Satz 1 sind

1. Personen, gegen die sich die Maßnahme richtet,
2. Adressaten der überwachten Postsendungen,
3. Inhaberinnen und Inhaber, Nutzerinnen und Nutzer der überwachten Telekommunikationsanschlüsse,
4. natürliche oder juristische Personen nach § 23a Abs. 4,
5. unvermeidbar betroffene Dritte gemäß § 23a Abs. 6 Satz 2.

Bei Betroffenen im Sinne von Satz 3 Nr. 2 bis 5 unterbleibt die Benachrichtigung, wenn sie nur mit unverhältnismäßigen Ermittlungen möglich wäre oder ihr überwiegende schutzwürdige Belange

anderer Betroffener entgegenstehen. Im Übrigen erfolgt die Benachrichtigung, sobald dies ohne Gefährdung des Untersuchungszwecks oder von Leben, Leib oder Freiheit einer Person oder von bedeutenden Vermögenswerten geschehen kann.

(5) Erfolgt die Benachrichtigung nicht binnen sechs Monaten nach Beendigung der Maßnahme, bedarf die weitere Zurückstellung der gerichtlichen Zustimmung. Die gerichtliche Zustimmung ist vorbehaltlich einer anderen gerichtlichen Anordnung jeweils nach sechs Monaten erneut einzuholen. Eine Benachrichtigung kann mit gerichtlicher Zustimmung endgültig unterbleiben, wenn die Voraussetzungen hierfür auf Dauer nicht vorliegen, im Falle des Absatzes 4 Satz 6 jedoch nicht vor Ablauf von fünf Jahren. 4§ 23b Abs. 3 gilt entsprechend. Ist die Benachrichtigung um insgesamt 18 Monate zurückgestellt worden, so ist das Oberlandesgericht zuständig, in dessen Bezirk das Zollkriminalamt seinen Sitz hat.

(6) Ist wegen desselben Sachverhalts ein strafrechtliches Verfahren eingeleitet worden, entscheidet die Staatsanwaltschaft nach Maßgabe der Regelungen der Strafprozessordnung über den Zeitpunkt der Benachrichtigung.

(7) Auch nach Erledigung einer in § 23a genannten Maßnahme können Betroffene binnen zwei Wochen nach ihrer Benachrichtigung die Überprüfung der Rechtmäßigkeit der Anordnung sowie der Art und Weise des Vollzugs beantragen. Über den Antrag entscheidet das Gericht, das für die Anordnung der Maßnahme zuständig gewesen ist. 3Gegen die Entscheidung ist die sofortige Beschwerde statthaft.

(8) Das Bundesministerium der Finanzen unterrichtet in Abständen von höchstens sechs Monaten ein Gremium, das aus neun vom Deutschen Bundestag bestimmten Abgeordneten besteht, über die Durchführung der §§ 23a bis 23f sowie §§ 45 und 46 dieses Gesetzes; dabei ist insbesondere über Anlass, Umfang, Dauer, Ergebnis, Kosten und Benachrichtigung Betroffener von im Berichtszeitraum durchgeführten Maßnahmen nach diesen Vorschriften zu berichten. Das Gremium erstattet dem Deutschen Bundestag nach Ablauf von drei Jahren nach Inkrafttreten dieser Vorschrift zusammenfassend zum Zwecke der Evaluierung einen die in Satz 1 genannten Angaben berücksichtigenden Bericht über die Durchführung der Maßnahmen.

§ 23d Übermittlungen durch das Zollkriminalamt

(1) Die vom Zollkriminalamt erlangten personenbezogenen Daten dürfen zur Verhütung von Straftaten an die mit polizeilichen Aufgaben betrauten Behörden übermittelt werden, wenn

1. tatsächliche Anhaltspunkte für den Verdacht bestehen, dass jemand

   a) Straftaten nach den §§ 80, 81 Abs. 1, § 94 Abs. 2, § 129a, auch in Verbindung mit § 129b Abs. 1, §§ 211, 212, 239a und 239b und 307 Abs. 1 bis 3 des Strafgesetzbuches oder

   b) Straftaten nach § 34 Abs. 1 bis 6, auch in Verbindung mit § 35 des Außenwirtschaftsgesetzes, §§ 19 bis 21 oder 22a Abs. 1 Nr. 4, 5 und 7 des Gesetzes über die Kontrolle von Kriegswaffen

   begehen will oder begeht oder

2. bestimmte Tatsachen den Verdacht begründen, dass jemand

   a) Straftaten, die in § 3 Abs. 1 Satz 1 Nr. 1 bis 5 und 7, Satz 2 des Artikel 10-Gesetzes bezeichnet sind, oder

   b) Straftaten nach den §§ 130, 146, 151 bis 152a, 181, 249 bis 251, 255, 261, 305a, 306 bis 306c, 308 Abs. 1 bis 4, § 309 Abs. 1 bis 5, §§ 313, 314, 315 Abs. 1, 3 oder Abs. 4, § 315b Abs. 3, §§ 316a, 316b Abs. 1 oder 3 oder § 316c Abs. 1 oder 3 des Strafgesetzbuches oder

   c) Straftaten nach § 29a Abs. 1 Nr. 2, § 30 Abs. 1 Nr. 1, 4 oder § 30a des Betäubungsmittelgesetzes

   begehen will oder begeht.

(2) Die Daten dürfen zur Verfolgung von Straftaten an die zuständigen Behörden übermittelt werden, wenn bestimmte Tatsachen den Verdacht begründen, dass jemand eine der in § 100a der

Strafprozessordnung genannten Straftaten begangen oder in Fällen, in denen der Versuch strafbar ist, zu begehen versucht hat oder durch eine Straftat vorbereitet hat.

(3) Die vom Zollkriminalamt erlangten personenbezogenen Daten dürfen an das Bundesamt für Wirtschaft und Ausfuhrkontrolle oder an das Bundesministerium für Wirtschaft und Technologie als Genehmigungsbehörde nach dem Gesetz über die Kontrolle von Kriegswaffen übermittelt werden, wenn bestimmte Tatsachen die Annahme begründen, dass die Kenntnis dieser Daten erforderlich ist

1. zur Aufklärung von Teilnehmern am Außenwirtschaftsverkehr über Umstände, die für die Einhaltung von Beschränkungen des Außenwirtschaftsverkehrs von Bedeutung sind, oder

2. im Rahmen eines Verfahrens zur Erteilung einer ausfuhrrechtlichen Genehmigung oder zur Unterrichtung von Teilnehmern am Außenwirtschaftsverkehr, soweit hierdurch eine Genehmigungspflicht für die Ausfuhr von Gütern begründet wird.

(4) Die vom Zollkriminalamt erlangten personenbezogenen Daten dürfen an die Verfassungsschutzbehörden des Bundes und der Länder sowie an den Militärischen Abschirmdienst übermittelt werden, wenn

1. tatsächliche Anhaltspunkte dafür bestehen, dass die Daten erforderlich sind zur Sammlung und Auswertung von Informationen über Bestrebungen in der Bundesrepublik Deutschland, die durch Anwendung von Gewalt oder darauf gerichtete Vorbereitungshandlungen gegen die in § 3 Abs. 1 Nr. 1, 3 und 4 des Bundesverfassungsschutzgesetzes genannten Schutzgüter gerichtet sind, oder

2. bestimmte Tatsachen den Verdacht sicherheitsgefährdender oder geheimdienstlicher Tätigkeiten für eine fremde Macht begründen.

(5) Die vom Zollkriminalamt erlangten personenbezogenen Daten dürfen an den Bundesnachrichtendienst übermittelt werden, wenn bestimmte Tatsachen den Verdacht begründen, dass diese Daten für die Erfüllung der Aufgaben des Bundesnachrichtendienstes nach § 1 Abs. 2 des Gesetzes über den Bundesnachrichtendienst zur Sammlung von Informationen über die in § 5 Abs. 1 Satz 3 Nr. 1 bis 3 des Artikel 10-Gesetzes genannten Gefahrenbereiche erforderlich sind.

(6) Die vom Zollkriminalamt erlangten personenbezogenen Daten dürfen zur Verhütung von Straftaten nach § 34 Abs. 1 bis 6, auch in Verbindung mit § 35 des Außenwirtschaftsgesetzes, oder nach den §§ 19 bis 21 oder 22a Abs. 1 Nr. 4, 5 und 7 des Gesetzes über die Kontrolle von Kriegswaffen an die mit der Ausfuhrabfertigung befassten Zolldienststellen der Mitgliedstaaten der Europäischen Union auf der Grundlage der zwischenstaatlichen Vereinbarungen über die gegenseitige Rechts- und Amtshilfe übermittelt werden, wenn tatsächliche Anhaltspunkte für den Verdacht bestehen, dass derartige Straftaten begangen werden sollen.

(7) Das Zollkriminalamt darf durch Maßnahmen nach § 23a Abs. 1, 3 und 4 erlangte personenbezogene Daten an die für die Verhütung oder Verfolgung von Straftaten zuständigen ausländischen öffentlichen sowie zwischen- und überstaatlichen Einrichtungen, die mit Aufgaben der Verhütung oder Verfolgung von Straftaten befasst sind, übermitteln, wenn

1. die Übermittlung zur Abwehr einer konkreten erheblichen Gefahr für außen- und sicherheitspolitische Belange der Bundesrepublik Deutschland oder erhebliche Sicherheitsinteressen des Empfängers erforderlich ist,

2. überwiegende schutzwürdige Interessen des Betroffenen nicht entgegenstehen und davon auszugehen ist, dass die Verwendung der Daten beim Empfänger in Einklang mit grundlegenden rechtsstaatlichen Prinzipien erfolgt, insbesondere ein angemessener Datenschutzstandard gewährleistet ist.

(8) Die Übermittlung nach den Absätzen 1 bis 7 ist nur zulässig, wenn sie zur Erfüllung der Aufgaben des Dritten, an den die Daten übermittelt werden, erforderlich ist. Sind mit personenbezogenen Daten, die übermittelt werden, weitere Daten des Betroffenen oder einer anderen Person in Akten so verbunden, dass eine Trennung nicht oder nur mit unvertretbarem Aufwand möglich ist, ist die Übermittlung auch dieser Daten zulässig; eine Nutzung dieser Daten

ist unzulässig. Die Verantwortung für die Zulässigkeit der Übermittlung trägt das Zollkriminalamt. Über die Übermittlung entscheidet ein Bediensteter des Zollkriminalamts, der die Befähigung zum Richteramt hat. 5Das Zollkriminalamt hat die Übermittlung und ihren Anlass zu protokollieren.

(9) Der Dritte, an den die Daten übermittelt werden, darf die Daten nur für die Zwecke verwenden, zu deren Erfüllung sie ihm übermittelt worden sind oder hätten übermittelt werden dürfen. Er prüft unverzüglich und sodann in Abständen von höchstens sechs Monaten, ob die übermittelten Daten für diese Zwecke erforderlich sind. Soweit die Daten für diese Zwecke nicht erforderlich sind, sind sie unverzüglich unter Aufsicht eines Bediensteten, der die Befähigung zum Richteramt hat, zu löschen. Die Löschung ist zu protokollieren. 5Bei Übermittlungen ins Ausland ist der Dritte, an den die Daten übermittelt werden, darauf hinzuweisen, dass die übermittelten Daten nur zu dem Zweck verwendet werden dürfen, zu dem sie übermittelt wurden, eine angebrachte Kennzeichnung beizubehalten ist und das Zollkriminalamt sich vorbehält, Auskunft über die Verwendung einzuholen.

§ 23e Verschwiegenheitspflicht

Werden Maßnahmen nach § 23a vorgenommen, so darf diese Tatsache von Personen, die geschäftsmäßig Post- oder Telekommunikationsdienste erbringen oder an der Erbringung solcher Dienste mitwirken, anderen nicht mitgeteilt werden.

§ 23f Entschädigung für Leistungen

Das Zollkriminalamt hat denjenigen, die geschäftsmäßig Post- oder Telekommunikationsdienste erbringen oder an der Erbringung solcher Dienste mitwirken, für ihre Leistungen bei der Durchführung von Maßnahmen nach § 23a eine Entschädigung zu gewähren, deren Umfang sich bei Maßnahmen zur

1. Überwachung der Post nach § 23 des Justizvergütungs- und -entschädigungsgesetzes und
2. Überwachung der Telekommunikation nach der Rechtsverordnung nach § 110 Abs. 9 des Telekommunikationsgesetzes

bemisst. Bis zum Inkrafttreten der Rechtsverordnung nach Satz 1 Nr. 2 bemisst sich die Entschädigung nach § 23 des Justizvergütungs- und -entschädigungsgesetzes.

§ 23g Erhebung von Verkehrsdaten

(1) 1Rechtfertigen Tatsachen die Annahme, dass Personen

1. Straftaten im Sinne des § 23a Abs. 1 vorbereiten oder
2. die öffentliche Sicherheit und Ordnung im Sinne des § 23a Abs. 3 erheblich gefährden,

darf das Zollkriminalamt auch ohne Wissen des Betroffenen Verkehrsdaten (§ 96 Abs. 1 des Telekommunikationsgesetzes) bei denjenigen, die geschäftsmäßig Telekommunikationsdienste erbringen oder daran mitwirken, erheben, soweit dies für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes der Person erforderlich ist. 2Die Erhebung von Standortdaten in Echtzeit ist zulässig.

(2) Die Anordnung darf sich nur gegen Personen im Sinne des § 23a Abs. 1, 3 oder 4 richten.

(3) Eine Maßnahme nach Absatz 1 darf nur durch das Gericht angeordnet werden, bei Gefahr im Verzug auch durch das Bundesministerium der Finanzen. Soweit die Anordnung nicht binnen drei Tagen durch das Gericht bestätigt wird, tritt sie außer Kraft. 3§ 23b Abs. 3 gilt entsprechend.

(4) Anordnungen nach Absatz 3 sind schriftlich zu erlassen und zu begründen. §23b Abs. 4 Satz 2 gilt entsprechend. Abweichend von § 23b Abs. 4 Satz 2 Nr. 2 genügt eine räumlich und zeitlich hinreichend bestimmte Bezeichnung der Telekommunikation, wenn die Erforschung des Sachverhalts auf andere Weise aussichtslos oder wesentlich erschwert wäre. Die Anordnung ist auf höchstens drei Monate zu befristen. Eine Verlängerung um jeweils bis zu drei Monaten ist zulässig, soweit die Voraussetzungen der Anordnung fortbestehen und die Maßnahme verhältnismäßig ist.

(5) Auf Grund der Anordnung hat jeder, der Telekommunikationsdienste erbringt oder daran mitwirkt (Diensteanbieter), dem Zollkriminalamt die Maßnahmen nach Absatz 1 zu ermöglichen und die erforderlichen Auskünfte zu erteilen. Ob und in welchem Umfang hierfür Vorkehrungen zu treffen sind, bestimmt sich nach dem Telekommunikationsgesetz und der Telekommunikations-Überwachungsverordnung.

(6) § 23c Abs. 2 bis 8 und die §§ 23d bis 23f gelten entsprechend.

REGNO UNITO

Regulation of Investigatory Powers Act 2000

Part I

Communications

Chapter I

Interception

Unlawful and authorised interception

Unlawful interception.

1. - (1) It shall be an offence for a person intentionally and without lawful authority to intercept, at any place in the United Kingdom, any communication in the course of its transmission by means of-

(a) a public postal service; or

(b) a public telecommunication system.

(2) It shall be an offence for a person-

(a) intentionally and without lawful authority, and

(b) otherwise than in circumstances in which his conduct is excluded by subsection (6) from criminal liability under this subsection,

to intercept, at any place in the United Kingdom, any communication in the course of its transmission by means of a private telecommunication system.

(3) Any interception of a communication which is carried out at any place in the United Kingdom by, or with the express or implied consent of, a person having the right to control the operation or the use of a private telecommunication system shall be actionable at the suit or instance of the sender or recipient, or intended recipient, of the communication if it is without lawful authority and is either-

(a) an interception of that communication in the course of its transmission by means of that private system; or

(b) an interception of that communication in the course of its transmission, by means of a public telecommunication system, to or from apparatus comprised in that private telecommunication system.

(4) Where the United Kingdom is a party to an international agreement which-

(a) relates to the provision of mutual assistance in connection with, or in the form of, the interception of communications,

(b) requires the issue of a warrant, order or equivalent instrument in cases in which assistance is given, and

(c) is designated for the purposes of this subsection by an order made by the Secretary of State,

it shall be the duty of the Secretary of State to secure that no request for assistance in accordance with the agreement is made on behalf of a person in the United Kingdom to the competent authorities of a country or territory outside the United Kingdom except with lawful authority.

(5) Conduct has lawful authority for the purposes of this section if, and only if-

(a) it is authorised by or under section 3 or 4;

(b) it takes place in accordance with a warrant under section 5 ("an interception warrant"); or

(c) it is in exercise, in relation to any stored communication, of any statutory power that is exercised (apart from this section) for the purpose of obtaining information or of taking possession of any document or other property;

and conduct (whether or not prohibited by this section) which has lawful authority for the purposes of this section by virtue of paragraph (a) or (b) shall also be taken to be lawful for all other purposes.

(6) The circumstances in which a person makes an interception of a communication in the course of its transmission by means of a private telecommunication system are such that his conduct is excluded from criminal liability under subsection (2) if-

(a) he is a person with a right to control the operation or the use of the system; or

(b) he has the express or implied consent of such a person to make the interception.

(7) A person who is guilty of an offence under subsection (1) or (2) shall be liable-

(a) on conviction on indictment, to imprisonment for a term not exceeding two years or to a fine, or to both;

(b) on summary conviction, to a fine not exceeding the statutory maximum.

(8) No proceedings for any offence which is an offence by virtue of this section shall be instituted-

(a) in England and Wales, except by or with the consent of the Director of Public Prosecutions;

(b) in Northern Ireland, except by or with the consent of the Director of Public Prosecutions for Northern Ireland.

Meaning and location of "interception" etc.

2. - (1) In this Act-

"postal service" means any service which-

(a) consists in the following, or in any one or more of them, namely, the collection, sorting, conveyance, distribution and delivery (whether in the United Kingdom or elsewhere) of postal items; and

(b) is offered or provided as a service the main purpose of which, or one of the main purposes of which, is to make available, or to facilitate, a means of transmission from place to place of postal items containing communications;

"private telecommunication system" means any telecommunication system which, without itself being a public telecommunication system, is a system in relation to which the following conditions are satisfied-

(a) it is attached, directly or indirectly and whether or not for the purposes of the communication in question, to a public telecommunication system; and

(b) there is apparatus comprised in the system which is both located in the United Kingdom and used (with or

without other apparatus) for making the attachment to the public telecommunication system;

"public postal service" means any postal service which is offered or provided to, or to a substantial section of, the public in any one or more parts of the United Kingdom;

"public telecommunications service" means any telecommunications service which is offered or provided to, or to a substantial section of, the public in any one or more parts of the United Kingdom;

"public telecommunication system" means any such parts of a telecommunication system by means of which any public telecommunications service is provided as are located in the United Kingdom;

"telecommunications service" means any service that consists in the provision of access to, and of facilities for making use of, any telecommunication system (whether or not one provided by the person providing the service); and

"telecommunication system" means any system (including the apparatus comprised in it) which exists (whether wholly or partly in the United Kingdom or elsewhere) for the purpose of facilitating the transmission of communications by any means involving the use of electrical or electro-magnetic energy.

(2) For the purposes of this Act, but subject to the following provisions of this section, a person intercepts a communication in the course of its transmission by means of a telecommunication system if, and only if, he-

(a) so modifies or interferes with the system, or its operation,

(b) so monitors transmissions made by means of the system, or

(c) so monitors transmissions made by wireless telegraphy to or from apparatus comprised in the system,

as to make some or all of the contents of the communication available, while being transmitted, to a person other than the sender or intended recipient of the communication.

(3) References in this Act to the interception of a communication do not include references to the interception of any communication broadcast for general reception.

(4) For the purposes of this Act the interception of a communication takes place in the United Kingdom if, and only if, the modification, interference or monitoring or, in the case of a postal item, the interception is effected by conduct within the United Kingdom and the communication is either-

(a) intercepted in the course of its transmission by means of a public postal service or public telecommunication system; or

(b) intercepted in the course of its transmission by means of a private telecommunication system in a case in which the sender or intended recipient of the communication is in the United Kingdom.

(5) References in this Act to the interception of a communication in the course of its transmission by means of a postal service or telecommunication system do not include references to-

(a) any conduct that takes place in relation only to so much of the communication as consists in any traffic data comprised in or attached to a communication (whether by the sender or otherwise) for the purposes of any postal service or telecommunication system by means of which it is being or may be transmitted; or

(b) any such conduct, in connection with conduct falling within paragraph (a), as gives a person who is neither the sender nor the intended recipient only so much access to a communication as is necessary for the purpose of identifying traffic data so comprised or attached.

(6) For the purposes of this section references to the modification of a telecommunication system include references to the attachment of any apparatus to, or other modification of or interference with-

(a) any part of the system; or

(b) any wireless telegraphy apparatus used for making transmissions to or from apparatus comprised in the system.

(7) For the purposes of this section the times while a communication is being transmitted by means of a telecommunication system shall be taken to include any time when the system by means of which the communication is being, or has been, transmitted is used for storing it in a manner that enables the intended recipient to collect it or otherwise to have access to it.

(8) For the purposes of this section the cases in which any contents of a communication are to be taken to be made available to a person while being transmitted shall include any case in which any of the contents of the communication, while being transmitted, are diverted or recorded so as to be available to a person subsequently.

(9) In this section "traffic data", in relation to any communication, means-

(a) any data identifying, or purporting to identify, any person, apparatus or location to or from which the communication is or may be transmitted,

(b) any data identifying or selecting, or purporting to identify or select, apparatus through which, or by means of which, the communication is or may be transmitted,

(c) any data comprising signals for the actuation of apparatus used for the purposes of a telecommunication system for effecting (in whole or in part) the transmission of any communication, and

(d) any data identifying the data or other data as data comprised in or attached to a particular communication,

but that expression includes data identifying a computer file or computer program access to which is obtained, or which is run, by means of the communication to the extent only that the file or program is identified by reference to the apparatus in which it is stored.

(10) In this section-

(a) references, in relation to traffic data comprising signals for the actuation of apparatus, to a telecommunication system by means of which a communication is being or may be transmitted include references to any telecommunication system in which that apparatus is comprised; and

(b) references to traffic data being attached to a communication include references to the data and the communication being logically associated with each other;

and in this section "data", in relation to a postal item, means anything written on the outside of the item.

(11) In this section "postal item" means any letter, postcard or other such thing in writing as may be used by the sender for imparting information to the recipient, or any packet or parcel.

Lawful interception without an interception warrant.

3. - (1) Conduct by any person consisting in the interception of a communication is authorised by this section if the communication is one which, or which that person has reasonable grounds for believing, is both-

(a) a communication sent by a person who has consented to the interception; and

(b) a communication the intended recipient of which has so consented.

(2) Conduct by any person consisting in the interception of a communication is authorised by this section if-

(a) the communication is one sent by, or intended for, a person who has consented to the interception; and

(b) surveillance by means of that interception has been authorised under Part II.

(3) Conduct consisting in the interception of a communication is authorised by this section if-

(a) it is conduct by or on behalf of a person who provides a postal service or a telecommunications service; and

(b) it takes place for purposes connected with the provision or operation of that service or with the enforcement, in relation to that service, of any enactment relating to the use of postal services or telecommunications services.

(4) Conduct by any person consisting in the interception of a communication in the course of its transmission by means of wireless telegraphy is authorised by this section if it takes place-

(a) with the authority of a designated person under section 5 of the Wireless Telegraphy Act 1949 (misleading messages and interception and disclosure of wireless telegraphy messages); and

(b) for purposes connected with anything falling within subsection (5).

(5) Each of the following falls within this subsection-

(a) the issue of licences under the Wireless Telegraphy Act 1949;

(b) the prevention or detection of anything which constitutes interference with wireless telegraphy; and

(c) the enforcement of any enactment contained in that Act or of any enactment not so contained that relates to such interference.

Power to provide for lawful interception.

4. - (1) Conduct by any person ("the interceptor") consisting in the interception of a communication in the course of its transmission by means of a telecommunication system is authorised by this section if-

(a) the interception is carried out for the purpose of obtaining information about the communications of a person who, or who the interceptor has reasonable grounds for believing, is in a country or territory outside the United Kingdom;

(b) the interception relates to the use of a telecommunications service provided to persons in that country or territory which is either-

(i) a public telecommunications service; or

(ii) a telecommunications service that would be a public telecommunications service if the persons to whom it is offered or provided were members of the public in a part of the United Kingdom;

(c) the person who provides that service (whether the interceptor or another person) is required by the law of that country or territory to carry out, secure or facilitate the

interception in question;

(d) the situation is one in relation to which such further conditions as may be prescribed by regulations made by the Secretary of State are required to be satisfied before conduct may be treated as authorised by virtue of this subsection; and

(e) the conditions so prescribed are satisfied in relation to that situation.

(2) Subject to subsection (3), the Secretary of State may by regulations authorise any such conduct described in the regulations as appears to him to constitute a legitimate practice reasonably required for the purpose, in connection with the carrying on of any business, of monitoring or keeping a record of-

(a) communications by means of which transactions are entered into in the course of that business; or

(b) other communications relating to that business or taking place in the course of its being carried on.

(3) Nothing in any regulations under subsection (2) shall authorise the interception of any communication except in the course of its transmission using apparatus or services provided by or to the person carrying on the business for use wholly or partly in connection with that business.

(4) Conduct taking place in a prison is authorised by this section if it is conduct in exercise of any power conferred by or under any rules made under section 47 of the Prison Act 1952, section 39 of the Prisons (Scotland) Act 1989 or section 13 of the Prison Act (Northern Ireland) 1953 (prison rules).

(5) Conduct taking place in any hospital premises where high security psychiatric services are provided is authorised by this section if it is conduct in pursuance of, and in accordance with, any direction given under section 17 of the National Health Service Act 1977 (directions as to the carrying out of their functions by health bodies) to the body providing those services at those premises.

(6) Conduct taking place in a state hospital is authorised by this section if it is conduct in pursuance of, and in accordance with, any direction given to the State Hospitals Board for Scotland under section 2(5) of the National Health Service (Scotland) Act 1978 (regulations and directions as to the exercise of their functions by health boards) as applied by Article 5(1) of and the Schedule to The State Hospitals Board for Scotland Order 1995 (which applies certain provisions of that Act of 1978 to the State Hospitals Board).

(7) In this section references to a business include references to any activities of a government department, of any public authority or of any person or office holder on whom functions are conferred by or under any enactment.

(8) In this section-

"government department" includes any part of the Scottish Administration, a Northern Ireland department and the National Assembly for Wales;

"high security psychiatric services" has the same meaning as in the National Health Service Act 1977;

"hospital premises" has the same meaning as in section 4(3) of that Act; and

"state hospital" has the same meaning as in the National Health Service (Scotland) Act 1978.

(9) In this section "prison" means-

(a) any prison, young offender institution, young offenders centre or remand centre which is under the general superintendence of, or is provided by, the Secretary of State under the Prison Act 1952 or the Prison Act (Northern Ireland) 1953, or

(b) any prison, young offenders institution or remand centre which is under the general superintendence of the Scottish Ministers under the Prisons (Scotland) Act 1989,

and includes any contracted out prison, within the meaning of Part IV of the Criminal Justice Act 1991 or section 106(4) of the Criminal Justice and Public Order Act 1994, and any legalised police cells within the meaning of section 14 of the Prisons (Scotland) Act 1989.

Interception with a warrant.

5. - (1) Subject to the following provisions of this Chapter, the Secretary of State may issue a warrant authorising or requiring the person to whom it is addressed, by any such conduct as may be described in the warrant, to secure any one or more of the following-

(a) the interception in the course of their transmission by means of a postal service or telecommunication system of the communications described in the warrant;

(b) the making, in accordance with an international mutual assistance agreement, of a request for the provision of such assistance in connection with, or in the form of, an interception of communications as may be so described;

(c) the provision, in accordance with an international mutual assistance agreement, to the competent authorities of a country or territory outside the United Kingdom of any such assistance in connection with, or in the form of, an interception of communications as may be so described;

(d) the disclosure, in such manner as may be so described, of intercepted material obtained by any interception authorised

or required by the warrant, and of related communications data.

(2) The Secretary of State shall not issue an interception warrant unless he believes-

(a) that the warrant is necessary on grounds falling within subsection (3); and

(b) that the conduct authorised by the warrant is proportionate to what is sought to be achieved by that conduct.

(3) Subject to the following provisions of this section, a warrant is necessary on grounds falling within this subsection if it is necessary-

(a) in the interests of national security;

(b) for the purpose of preventing or detecting serious crime;

(c) for the purpose of safeguarding the economic well-being of the United Kingdom; or

(d) for the purpose, in circumstances appearing to the Secretary of State to be equivalent to those in which he would issue a warrant by virtue of paragraph (b), of giving effect to the provisions of any international mutual assistance agreement.

(4) The matters to be taken into account in considering whether the requirements of subsection (2) are satisfied in the case of any warrant shall include whether the information which it is thought necessary to obtain under the warrant could reasonably be obtained by other means.

(5) A warrant shall not be considered necessary on the ground falling within subsection (3)(c) unless the information which it is thought necessary to obtain is information relating to the acts or intentions of persons outside the BritishIslands.

(6) The conduct authorised by an interception warrant shall be taken to include-

(a) all such conduct (including the interception of communications not identified by the warrant) as it is necessary to undertake in order to do what is expressly authorised or required by the warrant;

(b) conduct for obtaining related communications data; and

(c) conduct by any person which is conduct in pursuance of a requirement imposed by or on behalf of the person to whom the warrant is addressed to be provided with assistance with giving effect to the warrant.

Interception warrants

Application for issue of an interception

6. - (1) An interception warrant shall not be issued except on an application made by or on behalf of a person specified in subsection

warrant. (2).

(2) Those persons are-

(a) the Director-General of the Security Service;

(b) the Chief of the Secret Intelligence Service;

(c) the Director of GCHQ;

(d) the Director General of the National Criminal Intelligence Service;

(e) the Commissioner of Police of the Metropolis;

(f) the Chief Constable of the Royal Ulster Constabulary;

(g) the chief constable of any police force maintained under or by virtue of section 1 of the Police (Scotland) Act 1967;

(h) the Commissioners of Customs and Excise;

(i) the Chief of Defence Intelligence;

(j) a person who, for the purposes of any international mutual assistance agreement, is the competent authority of a country or territory outside the United Kingdom.

(3) An application for the issue of an interception warrant shall not be made on behalf of a person specified in subsection (2) except by a person holding office under the Crown.

Issue of warrants.

7. - (1) An interception warrant shall not be issued except-

(a) under the hand of the Secretary of State; or

(b) in a case falling within subsection (2), under the hand of a senior official.

(2) Those cases are-

(a) an urgent case in which the Secretary of State has himself expressly authorised the issue of the warrant in that case; and

(b) a case in which the warrant is for the purposes of a request for assistance made under an international mutual assistance agreement by the competent authorities of a country or territory outside the United Kingdom and either-

(i) it appears that the interception subject is outside the United Kingdom; or

(ii) the interception to which the warrant relates is to take place in relation only to premises outside the United Kingdom.

(3) An interception warrant-

(a) must be addressed to the person falling within section

6(2) by whom, or on whose behalf, the application for the warrant was made; and

(b) in the case of a warrant issued under the hand of a senior official, must contain, according to whatever is applicable-

(i) one of the statements set out in subsection (4); and

(ii) if it contains the statement set out in subsection (4)(b), one of the statements set out in subsection (5).

(4) The statements referred to in subsection (3)(b)(i) are-

(a) a statement that the case is an urgent case in which the Secretary of State has himself expressly authorised the issue of the warrant;

(b) a statement that the warrant is issued for the purposes of a request for assistance made under an international mutual assistance agreement by the competent authorities of a country or territory outside the United Kingdom.

(5) The statements referred to in subsection (3)(b)(ii) are-

(a) a statement that the interception subject appears to be outside the United Kingdom;

(b) a statement that the interception to which the warrant relates is to take place in relation only to premises outside the United Kingdom.

Contents of warrants.

8. - (1) An interception warrant must name or describe either-

(a) one person as the interception subject; or

(b) a single set of premises as the premises in relation to which the interception to which the warrant relates is to take place.

(2) The provisions of an interception warrant describing communications the interception of which is authorised or required by the warrant must comprise one or more schedules setting out the addresses, numbers, apparatus or other factors, or combination of factors, that are to be used for identifying the communications that may be or are to be intercepted.

(3) Any factor or combination of factors set out in accordance with subsection (2) must be one that identifies communications which are likely to be or to include-

(a) communications from, or intended for, the person named or described in the warrant in accordance with subsection (1); or

(b) communications originating on, or intended for

transmission to, the premises so named or described.

(4) Subsections (1) and (2) shall not apply to an interception warrant if-

(a) the description of communications to which the warrant relates confines the conduct authorised or required by the warrant to conduct falling within subsection (5); and

(b) at the time of the issue of the warrant, a certificate applicable to the warrant has been issued by the Secretary of State certifying-

(i) the descriptions of intercepted material the examination of which he considers necessary; and

(ii) that he considers the examination of material of those descriptions necessary as mentioned in section 5(3)(a), (b) or (c).

(5) Conduct falls within this subsection if it consists in-

(a) the interception of external communications in the course of their transmission by means of a telecommunication system; and

(b) any conduct authorised in relation to any such interception by section 5(6).

(6) A certificate for the purposes of subsection (4) shall not be issued except under the hand of the Secretary of State.

Duration, cancellation and renewal of warrants.

9. - (1) An interception warrant-

(a) shall cease to have effect at the end of the relevant period; but

(b) may be renewed, at any time before the end of that period, by an instrument under the hand of the Secretary of State or, in a case falling within section 7(2)(b), under the hand of a senior official.

(2) An interception warrant shall not be renewed under subsection (1) unless the Secretary of State believes that the warrant continues to be necessary on grounds falling within section 5(3).

(3) The Secretary of State shall cancel an interception warrant if he is satisfied that the warrant is no longer necessary on grounds falling within section 5(3).

(4) The Secretary of State shall cancel an interception warrant if, at any time before the end of the relevant period, he is satisfied in a case in which-

(a) the warrant is one which was issued containing the statement set out in section 7(5)(a) or has been renewed by an instrument containing the statement set out in subsection (5)(b)(i) of this section, and

(b) the latest renewal (if any) of the warrant is not a renewal by an instrument under the hand of the Secretary of State,

that the person named or described in the warrant as the interception subject is in the United Kingdom.

(5) An instrument under the hand of a senior official that renews an interception warrant must contain-

(a) a statement that the renewal is for the purposes of a request for assistance made under an international mutual assistance agreement by the competent authorities of a country or territory outside the United Kingdom; and

(b) whichever of the following statements is applicable-

(i) a statement that the interception subject appears to be outside the United Kingdom;

(ii) a statement that the interception to which the warrant relates is to take place in relation only to premises outside the United Kingdom.

(6) In this section "the relevant period"-

(a) in relation to an unrenewed warrant issued in a case falling within section 7(2)(a) under the hand of a senior official, means the period ending with the fifth working day following the day of the warrant's issue;

(b) in relation to a renewed warrant the latest renewal of which was by an instrument endorsed under the hand of the Secretary of State with a statement that the renewal is believed to be necessary on grounds falling within section 5(3)(a) or (c), means the period of six months beginning with the day of the warrant's renewal; and

(c) in all other cases, means the period of three months beginning with the day of the warrant's issue or, in the case of a warrant that has been renewed, of its latest renewal.

Modification of warrants and certificates.

10. - (1) The Secretary of State may at any time-

(a) modify the provisions of an interception warrant; or

(b) modify a section 8(4) certificate so as to include in the certified material any material the examination of which he considers to be necessary as mentioned in section 5(3)(a), (b) or (c).

(2) If at any time the Secretary of State considers that any factor set out in a schedule to an interception warrant is no longer relevant for identifying communications which, in the case of that warrant, are likely to be or to include communications falling within section 8(3)(a) or (b), it shall be his duty to modify the warrant by the deletion of that factor.

(3) If at any time the Secretary of State considers that the material certified by a section 8(4) certificate includes any material the examination of which is no longer necessary as mentioned in any of paragraphs (a) to (c) of section 5(3), he shall modify the certificate so as to exclude that material from the certified material.

(4) Subject to subsections (5) to (8), a warrant or certificate shall not be modified under this section except by an instrument under the hand of the Secretary of State or of a senior official.

(5) Unscheduled parts of an interception warrant shall not be modified under the hand of a senior official except in an urgent case in which-

(a) the Secretary of State has himself expressly authorised the modification; and

(b) a statement of that fact is endorsed on the modifying instrument.

(6) Subsection (4) shall not authorise the making under the hand of either-

(a) the person to whom the warrant is addressed, or

(b) any person holding a position subordinate to that person,

of any modification of any scheduled parts of an interception warrant.

(7) A section 8(4) certificate shall not be modified under the hand of a senior official except in an urgent case in which-

(a) the official in question holds a position in respect of which he is expressly authorised by provisions contained in the certificate to modify the certificate on the Secretary of State's behalf; or

(b) the Secretary of State has himself expressly authorised the modification and a statement of that fact is endorsed on the modifying instrument.

(8) Where modifications in accordance with this subsection are expressly authorised by provision contained in the warrant, the scheduled parts of an interception warrant may, in an urgent case, be modified by an instrument under the hand of-

(a) the person to whom the warrant is addressed; or

(b) a person holding any such position subordinate to that person as may be identified in the provisions of the warrant.

(9) Where-

(a) a warrant or certificate is modified by an instrument under the hand of a person other than the Secretary of State, and

(b) a statement for the purposes of subsection (5)(b) or (7)(b) is endorsed on the instrument, or the modification is made under subsection (8),

that modification shall cease to have effect at the end of the fifth working day following the day of the instrument's issue.

(10) For the purposes of this section-

(a) the scheduled parts of an interception warrant are any provisions of the warrant that are contained in a schedule of identifying factors comprised in the warrant for the purposes of section 8(2); and

(b) the modifications that are modifications of the scheduled parts of an interception warrant include the insertion of an additional such schedule in the warrant;

and references in this section to unscheduled parts of an interception warrant, and to their modification, shall be construed accordingly.

Implementation of warrants.

11. - (1) Effect may be given to an interception warrant either-

(a) by the person to whom it is addressed; or

(b) by that person acting through, or together with, such other persons as he may require (whether under subsection (2) or otherwise) to provide him with assistance with giving effect to the warrant.

(2) For the purpose of requiring any person to provide assistance in relation to an interception warrant the person to whom it is addressed may-

(a) serve a copy of the warrant on such persons as he considers may be able to provide such assistance; or

(b) make arrangements under which a copy of it is to be or may be so served.

(3) The copy of an interception warrant that is served on any person under subsection (2) may, to the extent authorised-

(a) by the person to whom the warrant is addressed, or

(b) by the arrangements made by him for the purposes of that subsection,

omit any one or more of the schedules to the warrant.

(4) Where a copy of an interception warrant has been served by or on behalf of the person to whom it is addressed on-

(a) a person who provides a postal service,

(b) a person who provides a public telecommunications service, or

(c) a person not falling within paragraph (b) who has control of the whole or any part of a telecommunication system located wholly or partly in the United Kingdom,

it shall (subject to subsection (5)) be the duty of that person to take all such steps for giving effect to the warrant as are notified to him by or on behalf of the person to whom the warrant is addressed.

(5) A person who is under a duty by virtue of subsection (4) to take steps for giving effect to a warrant shall not be required to take any steps which it is not reasonably practicable for him to take.

(6) For the purposes of subsection (5) the steps which it is reasonably practicable for a person to take in a case in which obligations have been imposed on him by or under section 12 shall include every step which it would have been reasonably practicable for him to take had he complied with all the obligations so imposed on him.

(7) A person who knowingly fails to comply with his duty under subsection (4) shall be guilty of an offence and liable-

(a) on conviction on indictment, to imprisonment for a term not exceeding two years or to a fine, or to both;

(b) on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum, or to both.

(8) A person's duty under subsection (4) to take steps for giving effect to a warrant shall be enforceable by civil proceedings by the Secretary of State for an injunction, or for specific performance of a statutory duty under section 45 of the Court of Session Act 1988, or for any other appropriate relief.

(9) For the purposes of this Act the provision of assistance with giving effect to an interception warrant includes any disclosure to the person to whom the warrant is addressed, or to persons acting on his behalf, of intercepted material obtained by any interception authorised or required by the warrant, and of any related communications data.

Interception capability and costs

Maintenance of interception capability.

12. - (1) The Secretary of State may by order provide for the imposition by him on persons who-

(a) are providing public postal services or public telecommunications services, or

(b) are proposing to do so,

of such obligations as it appears to him reasonable to impose for the purpose of securing that it is and remains practicable for requirements to provide assistance in relation to interception warrants to be imposed and complied with.

(2) The Secretary of State's power to impose the obligations provided for by an order under this section shall be exercisable by the giving, in accordance with the order, of a notice requiring the person who is to be subject to the obligations to take all such steps as may be specified or described in the notice.

(3) Subject to subsection (11), the only steps that may be specified or described in a notice given to a person under subsection (2) are steps appearing to the Secretary of State to be necessary for securing that that person has the practical capability of providing any assistance which he may be required to provide in relation to relevant interception warrants.

(4) A person shall not be liable to have an obligation imposed on him in accordance with an order under this section by reason only that he provides, or is proposing to provide, to members of the public a telecommunications service the provision of which is or, as the case may be, will be no more than-

(a) the means by which he provides a service which is not a telecommunications service; or

(b) necessarily incidental to the provision by him of a service which is not a telecommunications service.

(5) Where a notice is given to any person under subsection (2) and otherwise than by virtue of subsection (6)(c), that person may, before the end of such period as may be specified in an order under this section, refer the notice to the Technical Advisory Board.

(6) Where a notice given to any person under subsection (2) is referred to the Technical Advisory Board under subsection (5)-

(a) there shall be no requirement for that person to comply, except in pursuance of a notice under paragraph (c)(ii), with any obligations imposed by the notice;

(b) the Board shall consider the technical requirements and

the financial consequences, for the person making the reference, of the notice referred to them and shall report their conclusions on those matters to that person and to the Secretary of State; and

(c) the Secretary of State, after considering any report of the Board relating to the notice, may either-

(i) withdraw the notice; or

(ii) give a further notice under subsection (2) confirming its effect, with or without modifications.

(7) It shall be the duty of a person to whom a notice is given under subsection (2) to comply with the notice; and that duty shall be enforceable by civil proceedings by the Secretary of State for an injunction, or for specific performance of a statutory duty under section 45 of the Court of Session Act 1988, or for any other appropriate relief.

(8) A notice for the purposes of subsection (2) must specify such period as appears to the Secretary of State to be reasonable as the period within which the steps specified or described in the notice are to be taken.

(9) Before making an order under this section the Secretary of State shall consult with-

(a) such persons appearing to him to be likely to be subject to the obligations for which it provides,

(b) the Technical Advisory Board,

(c) such persons representing persons falling within paragraph (a), and

(d) such persons with statutory functions in relation to persons falling within that paragraph,

as he considers appropriate.

(10) The Secretary of State shall not make an order under this section unless a draft of the order has been laid before Parliament and approved by a resolution of each House.

(11) For the purposes of this section the question whether a person has the practical capability of providing assistance in relation to relevant interception warrants shall include the question whether all such arrangements have been made as the Secretary of State considers necessary-

(a) with respect to the disclosure of intercepted material;

(b) for the purpose of ensuring that security and confidentiality are maintained in relation to, and to matters connected with, the provision of any such assistance; and

(c) for the purpose of facilitating the carrying out of any

functions in relation to this Chapter of the Interception of Communications Commissioner;

but before determining for the purposes of the making of any order, or the imposition of any obligation, under this section what arrangements he considers necessary for the purpose mentioned in paragraph (c) the Secretary of State shall consult that Commissioner.

(12) In this section "relevant interception warrant"-

(a) in relation to a person providing a public postal service, means an interception warrant relating to the interception of communications in the course of their transmission by means of that service; and

(b) in relation to a person providing a public telecommunications service, means an interception warrant relating to the interception of communications in the course of their transmission by means of a telecommunication system used for the purposes of that service.

Technical Advisory Board.

13. - (1) There shall be a Technical Advisory Board consisting of such number of persons appointed by the Secretary of State as he may by order provide.

(2) The order providing for the membership of the Technical Advisory Board must also make provision which is calculated to ensure-

(a) that the membership of the Technical Advisory Board includes persons likely effectively to represent the interests of the persons on whom obligations may be imposed under section 12;

(b) that the membership of the Board includes persons likely effectively to represent the interests of the persons by or on whose behalf applications for interception warrants may be made;

(c) that such other persons (if any) as the Secretary of State thinks fit may be appointed to be members of the Board; and

(d) that the Board is so constituted as to produce a balance between the representation of the interests mentioned in paragraph (a) and the representation of those mentioned in paragraph (b).

(3) The Secretary of State shall not make an order under this section unless a draft of the order has been laid before Parliament and approved by a resolution of each House.

Grants for

14. - (1) It shall be the duty of the Secretary of State to ensure

interception costs.

that such arrangements are in force as are necessary for securing that a person who provides-

(a) a postal service, or

(b) a telecommunications service,

receives such contribution as is, in the circumstances of that person's case, a fair contribution towards the costs incurred, or likely to be incurred, by that person in consequence of the matters mentioned in subsection (2).

(2) Those matters are-

(a) in relation to a person providing a postal service, the issue of interception warrants relating to communications transmitted by means of that postal service;

(b) in relation to a person providing a telecommunications service, the issue of interception warrants relating to communications transmitted by means of a telecommunication system used for the purposes of that service;

(c) in relation to each description of person, the imposition on that person of obligations provided for by an order under section 12.

(3) For the purpose of complying with his duty under this section, the Secretary of State may make arrangements for payments to be made out of money provided by Parliament.

Restrictions on use of intercepted material etc.

General safeguards.

15. - (1) Subject to subsection (6), it shall be the duty of the Secretary of State to ensure, in relation to all interception warrants, that such arrangements are in force as he considers necessary for securing-

(a) that the requirements of subsections (2) and (3) are satisfied in relation to the intercepted material and any related communications data; and

(b) in the case of warrants in relation to which there are section 8(4) certificates, that the requirements of section 16 are also satisfied.

(2) The requirements of this subsection are satisfied in relation to the intercepted material and any related communications data if each of the following-

(a) the number of persons to whom any of the material or data is disclosed or otherwise made available,

(b) the extent to which any of the material or data is disclosed or otherwise made available,

(c) the extent to which any of the material or data is copied, and

(d) the number of copies that are made,

is limited to the minimum that is necessary for the authorised purposes.

(3) The requirements of this subsection are satisfied in relation to the intercepted material and any related communications data if each copy made of any of the material or data (if not destroyed earlier) is destroyed as soon as there are no longer any grounds for retaining it as necessary for any of the authorised purposes.

(4) For the purposes of this section something is necessary for the authorised purposes if, and only if-

(a) it continues to be, or is likely to become, necessary as mentioned in section 5(3);

(b) it is necessary for facilitating the carrying out of any of the functions under this Chapter of the Secretary of State;

(c) it is necessary for facilitating the carrying out of any functions in relation to this Part of the Interception of Communications Commissioner or of the Tribunal;

(d) it is necessary to ensure that a person conducting a criminal prosecution has the information he needs to determine what is required of him by his duty to secure the fairness of the prosecution; or

(e) it is necessary for the performance of any duty imposed on any person by the Public Records Act 1958 or the Public Records Act (Northern Ireland) 1923.

(5) The arrangements for the time being in force under this section for securing that the requirements of subsection (2) are satisfied in relation to the intercepted material or any related communications data must include such arrangements as the Secretary of State considers necessary for securing that every copy of the material or data that is made is stored, for so long as it is retained, in a secure manner.

(6) Arrangements in relation to interception warrants which are made for the purposes of subsection (1)-

(a) shall not be required to secure that the requirements of subsections (2) and (3) are satisfied in so far as they relate to any of the intercepted material or related communications data, or any copy of any such material or data, possession of which has been surrendered to any authorities of a country or territory outside the United Kingdom; but

(b) shall be required to secure, in the case of every such warrant, that possession of the intercepted material and data

and of copies of the material or data is surrendered to authorities of a country or territory outside the United Kingdom only if the requirements of subsection (7) are satisfied.

(7) The requirements of this subsection are satisfied in the case of a warrant if it appears to the Secretary of State-

(a) that requirements corresponding to those of subsections (2) and (3) will apply, to such extent (if any) as the Secretary of State thinks fit, in relation to any of the intercepted material or related communications data possession of which, or of any copy of which, is surrendered to the authorities in question; and

(b) that restrictions are in force which would prevent, to such extent (if any) as the Secretary of State thinks fit, the doing of anything in, for the purposes of or in connection with any proceedings outside the United Kingdom which would result in such a disclosure as, by virtue of section 17, could not be made in the United Kingdom.

(8) In this section "copy", in relation to intercepted material or related communications data, means any of the following (whether or not in documentary form)-

(a) any copy, extract or summary of the material or data which identifies itself as the product of an interception, and

(b) any record referring to an interception which is a record of the identities of the persons to or by whom the intercepted material was sent, or to whom the communications data relates,

and "copied" shall be construed accordingly.

Extra safeguards in the case of certificated warrants.

16. - (1) For the purposes of section 15 the requirements of this section, in the case of a warrant in relation to which there is a section 8(4) certificate, are that the intercepted material is read, looked at or listened to by the persons to whom it becomes available by virtue of the warrant to the extent only that it-

(a) has been certified as material the examination of which is necessary as mentioned in section 5(3)(a), (b) or (c); and

(b) falls within subsection (2).

(2) Subject to subsections (3) and (4), intercepted material falls within this subsection so far only as it is selected to be read, looked at or listened to otherwise than according to a factor which-

(a) is referable to an individual who is known to be for the time being in the BritishIslands; and

(b) has as its purpose, or one of its purposes, the identification of material contained in communications sent by him, or intended for him.

(3) Intercepted material falls within subsection (2), notwithstanding that it is selected by reference to any such factor as is mentioned in paragraph (a) and (b) of that subsection, if-

(a) it is certified by the Secretary of State for the purposes of section 8(4) that the examination of material selected according to factors referable to the individual in question is necessary as mentioned in subsection 5(3)(a), (b) or (c); and

(b) the material relates only to communications sent during a period of not more than three months specified in the certificate.

(4) Intercepted material also falls within subsection (2), notwithstanding that it is selected by reference to any such factor as is mentioned in paragraph (a) and (b) of that subsection, if-

(a) the person to whom the warrant is addressed believes, on reasonable grounds, that the circumstances are such that the material would fall within that subsection; or

(b) the conditions set out in subsection (5) below are satisfied in relation to the selection of the material.

(5) Those conditions are satisfied in relation to the selection of intercepted material if-

(a) it has appeared to the person to whom the warrant is addressed that there has been such a relevant change of circumstances as, but for subsection (4)(b), would prevent the intercepted material from falling within subsection (2);

(b) since it first so appeared, a written authorisation to read, look at or listen to the material has been given by a senior official; and

(c) the selection is made before the end of the first working day after the day on which it first so appeared to that person.

(6) References in this section to its appearing that there has been a relevant change of circumstances are references to its appearing either-

(a) that the individual in question has entered the BritishIslands; or

(b) that a belief by the person to whom the warrant is addressed in the individual's presence outside the BritishIslands was in fact mistaken.

Exclusion of matters from legal proceedings.

17. - (1) Subject to section 18, no evidence shall be adduced, question asked, assertion or disclosure made or other thing done in, for the purposes of or in connection with any legal proceedings which (in any manner)-

(a) discloses, in circumstances from which its origin in anything falling within subsection (2) may be inferred, any of the contents of an intercepted communication or any related communications data; or

(b) tends (apart from any such disclosure) to suggest that anything falling within subsection (2) has or may have occurred or be going to occur.

(2) The following fall within this subsection-

(a) conduct by a person falling within subsection (3) that was or would be an offence under section 1(1) or (2) of this Act or under section 1 of the Interception of Communications Act 1985;

(b) a breach by the Secretary of State of his duty under section 1(4) of this Act;

(c) the issue of an interception warrant or of a warrant under the Interception of Communications Act 1985;

(d) the making of an application by any person for an interception warrant, or for a warrant under that Act;

(e) the imposition of any requirement on any person to provide assistance with giving effect to an interception warrant.

(3) The persons referred to in subsection (2)(a) are-

(a) any person to whom a warrant under this Chapter may be addressed;

(b) any person holding office under the Crown;

(c) any member of the National Criminal Intelligence Service;

(d) any member of the National Crime Squad;

(e) any person employed by or for the purposes of a police force;

(f) any person providing a postal service or employed for the purposes of any business of providing such a service; and

(g) any person providing a public telecommunications service or employed for the purposes of any business of providing such a service.

(4) In this section "intercepted communication" means any communication intercepted in the course of its transmission by means of a postal service or telecommunication system.

Exceptions to section 17.

18. - (1) Section 17(1) shall not apply in relation to-

(a) any proceedings for a relevant offence;

(b) any civil proceedings under section 11(8);

(c) any proceedings before the Tribunal;

(d) any proceedings on an appeal or review for which provision is made by an order under section 67(8);

(e) any proceedings before the Special Immigration Appeals Commission or any proceedings arising out of proceedings before that Commission; or

(f) any proceedings before the Proscribed Organisations Appeal Commission or any proceedings arising out of proceedings before that Commission.

(2) Subsection (1) shall not, by virtue of paragraph (e) or (f), authorise the disclosure of anything-

(a) in the case of any proceedings falling within paragraph (e), to-

(i) the appellant to the Special Immigration Appeals Commission; or

(ii) any person who for the purposes of any proceedings so falling (but otherwise than by virtue of an appointment under section 6 of the Special Immigration Appeals Commission Act 1997) represents that appellant;

or

(b) in the case of proceedings falling within paragraph (f), to-

(i) the applicant to the Proscribed Organisations Appeal Commission;

(ii) the organisation concerned (if different);

(iii) any person designated under paragraph 6 of Schedule 3 to the Terrorism Act 2000 to conduct proceedings so falling on behalf of that organisation; or

(iv) any person who for the purposes of any proceedings so falling (but otherwise than by virtue of an appointment under paragraph 7 of that Schedule) represents that applicant or that organisation.

(3) Section 17(1) shall not prohibit anything done in, for the purposes of, or in connection with, so much of any legal proceedings as relates to the fairness or unfairness of a dismissal on the grounds of any conduct constituting an offence under section 1(1) or (2), 11(7) or 19 of this Act, or section 1 of the Interception of Communications Act 1985.

(4) Section 17(1)(a) shall not prohibit the disclosure of any of the contents of a communication if the interception of that communication was lawful by virtue of section 1(5)(c), 3 or 4.

(5) Where any disclosure is proposed to be or has been made on the grounds that it is authorised by subsection (4), section 17(1) shall not prohibit the doing of anything in, or for the purposes of, so much of any legal proceedings as relates to the question whether that

disclosure is or was so authorised.

(6) Section 17(1)(b) shall not prohibit the doing of anything that discloses any conduct of a person for which he has been convicted of an offence under section 1(1) or (2), 11(7) or 19 of this Act, or section 1 of the Interception of Communications Act 1985.

(7) Nothing in section 17(1) shall prohibit any such disclosure of any information that continues to be available for disclosure as is confined to-

(a) a disclosure to a person conducting a criminal prosecution for the purpose only of enabling that person to determine what is required of him by his duty to secure the fairness of the prosecution; or

(b) a disclosure to a relevant judge in a case in which that judge has ordered the disclosure to be made to him alone.

(8) A relevant judge shall not order a disclosure under subsection (7)(b) except where he is satisfied that the exceptional circumstances of the case make the disclosure essential in the interests of justice.

(9) Subject to subsection (10), where in any criminal proceedings-

(a) a relevant judge does order a disclosure under subsection (7)(b), and

(b) in consequence of that disclosure he is of the opinion that there are exceptional circumstances requiring him to do so,

he may direct the person conducting the prosecution to make for the purposes of the proceedings any such admission of fact as that judge thinks essential in the interests of justice.

(10) Nothing in any direction under subsection (9) shall authorise or require anything to be done in contravention of section 17(1).

(11) In this section "a relevant judge" means-

(a) any judge of the High Court or of the Crown Court or any Circuit judge;

(b) any judge of the High Court of Justiciary or any sheriff;

(c) in relation to a court-martial, the judge advocate appointed in relation to that court-martial under section 84B of the Army Act 1955, section 84B of the Air Force Act 1955 or section 53B of the Naval Discipline Act 1957; or

(d) any person holding any such judicial office as entitles him to exercise the jurisdiction of a judge falling within paragraph (a) or (b).

(12) In this section "relevant offence" means-

(a) an offence under any provision of this Act;

(b) an offence under section 1 of the Interception of Communications Act 1985;

(c) an offence under section 5 of the Wireless Telegraphy Act 1949;

(d) an offence under section 45 of the Telegraph Act 1863, section 20 of the Telegraph Act 1868 or section 58 of the Post Office Act 1953;

(e) an offence under section 45 of the Telecommunications Act 1984;

(f) an offence under section 4 of the Official Secrets Act 1989 relating to any such information, document or article as is mentioned in subsection (3)(a) of that section;

(g) an offence under section 1 or 2 of the Official Secrets Act 1911 relating to any sketch, plan, model, article, note, document or information which incorporates or relates to the contents of any intercepted communication or any related communications data or tends to suggest as mentioned in section 17(1)(b) of this Act;

(h) perjury committed in the course of any proceedings mentioned in subsection (1) or (3) of this section;

(i) attempting or conspiring to commit, or aiding, abetting, counselling or procuring the commission of, an offence falling within any of the preceding paragraphs; and

(j) contempt of court committed in the course of, or in relation to, any proceedings mentioned in subsection (1) or (3) of this section.

(13) In subsection (12) "intercepted communication" has the same meaning as in section 17.

Offence for unauthorised disclosures.

19. - (1) Where an interception warrant has been issued or renewed, it shall be the duty of every person falling within subsection (2) to keep secret all the matters mentioned in subsection (3).

(2) The persons falling within this subsection are-

(a) the persons specified in section 6(2);

(b) every person holding office under the Crown;

(c) every member of the National Criminal Intelligence Service;

(d) every member of the National Crime Squad;

(e) every person employed by or for the purposes of a police force;

(f) persons providing postal services or employed for the

purposes of any business of providing such a service;

(g) persons providing public telecommunications services or employed for the purposes of any business of providing such a service;

(h) persons having control of the whole or any part of a telecommunication system located wholly or partly in the United Kingdom.

(3) Those matters are-

(a) the existence and contents of the warrant and of any section 8(4) certificate in relation to the warrant;

(b) the details of the issue of the warrant and of any renewal or modification of the warrant or of any such certificate;

(c) the existence and contents of any requirement to provide assistance with giving effect to the warrant;

(d) the steps taken in pursuance of the warrant or of any such requirement; and

(e) everything in the intercepted material, together with any related communications data.

(4) A person who makes a disclosure to another of anything that he is required to keep secret under this section shall be guilty of an offence and liable-

(a) on conviction on indictment, to imprisonment for a term not exceeding five years or to a fine, or to both;

(b) on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum, or to both.

(5) In proceedings against any person for an offence under this section in respect of any disclosure, it shall be a defence for that person to show that he could not reasonably have been expected, after first becoming aware of the matter disclosed, to take steps to prevent the disclosure.

(6) In proceedings against any person for an offence under this section in respect of any disclosure, it shall be a defence for that person to show that-

(a) the disclosure was made by or to a professional legal adviser in connection with the giving, by the adviser to any client of his, of advice about the effect of provisions of this Chapter; and

(b) the person to whom or, as the case may be, by whom it was made was the client or a representative of the client.

(7) In proceedings against any person for an offence under this section in respect of any disclosure, it shall be a defence for that person to show that the disclosure was made by a legal adviser-

(a) in contemplation of, or in connection with, any legal proceedings; and

(b) for the purposes of those proceedings.

(8) Neither subsection (6) nor subsection (7) applies in the case of a disclosure made with a view to furthering any criminal purpose.

(9) In proceedings against any person for an offence under this section in respect of any disclosure, it shall be a defence for that person to show that the disclosure was confined to a disclosure made to the Interception of Communications Commissioner or authorised-

(a) by that Commissioner;

(b) by the warrant or the person to whom the warrant is or was addressed;

(c) by the terms of the requirement to provide assistance; or

(d) by section 11(9).

Interpretation of Chapter I

Interpretation of Chapter I.

20. In this Chapter-

"certified", in relation to a section 8(4) certificate, means of a description certified by the certificate as a description of material the examination of which the Secretary of State considers necessary;

"external communication" means a communication sent or received outside the BritishIslands;

"intercepted material", in relation to an interception warrant, means the contents of any communications intercepted by an interception to which the warrant relates;

"the interception subject", in relation to an interception warrant, means the person about whose communications information is sought by the interception to which the warrant relates;

"international mutual assistance agreement" means an international agreement designated for the purposes of section 1(4);

"related communications data", in relation to a communication intercepted in the course of its transmission by means of a postal service or telecommunication system, means so much of any communications data (within the meaning of Chapter II of this Part) as-

(a) is obtained by, or in connection with, the interception; and

(b) relates to the communication or to the sender or

recipient, or intended recipient, of the communication;

"section 8(4) certificate" means any certificate issued for the purposes of section 8(4).

SPAGNA

Costituzione

Articolo 18

1. E’ garantito il diritto all’onore, all’intimità personale e familiare e alla propria immagine.

2. Il domicilio è inviolabile. Nessun accesso o perquisizione saranno consentiti senza il consenso del titolare o decisione giudizaria, eccezion fatta nel caso di flagrante reato.

3. E’ garantito il segreto delle comunicazioni e in specie di quelle postali, telegrafiche e telefoniche, salvo decisione giudiziale.

4. La legge porrà limiti all’uso dell’informatica per salvaguardare l’onore e l’intimità personale e familiare dei cittadini e il pieno esercizio dei loro diritti.

Artículo 579.

Modificado por Ley Orgánica 4/1988

1. Podrá el Juez acordar la detención de la correspondencia privada, postal y telegráfica que el procesado remitiere o recibiere y su apertura y examen, si hubiere indicios de obtener por estos medios el descubrimiento o la comprobación de algún hecho o circunstancia importante de la causa.

2. Asimismo, el Juez podrá acordar, en resolución motivada, la intervención de las comunicaciones telefónicas del procesado, si hubiere indicios de obtener por estos medios el descubrimiento o la comprobación de algún hecho o circunstancia importante de la causa.

3. De igual forma, el Juez podrá acordar, en resolución motivada, por un plazo de hasta tres meses, prorrogable por iguales períodos, la observación le las comunicaciones postales, telegráficas o telefónicas de las personas obre las que existan indicios de responsabilidad criminal, así como de las comunicaciones de las que se sirvan para la realización de sus fines delictivos.

4. En caso de urgencia, cuando las investigaciones se realicen para la averiguación de delitos relacionados con la actuación de bandas armadas elementos terroristas o rebeldes, la medida prevista en el número 3 de este artículo podrá ordenarla el Ministro del Interior o, en su defecto, el Director de la Seguridad del Estado, comunicándolo inmediatamente por escrito motivado al Juez competente, quien, también de forma motivada, revocará o confirmará tal resolución en un plazo máximo de setenta y dos oras desde que fue ordenada la observación.

---

[1] Il testo del *Décret n°2006-1405 du 17 novembre 2006 modifiant le décret n° 64-754 du 25 juillet 1964 relatif à l'organisation du ministère de la justice et instituant une délégation aux interceptions judiciaires* è consultabile all'indirizzo: http://www.legifrance.gouv.fr/./affichTexte.do?cidTexte=JORFTEXT000000641157&dateTexte=20080618&fastPos=1&fastReqId=1697720642&oldAction=rechTexte

[2] Il XVI° Rapporto della Commissione, relativo al 2007 e pubblicato nel 2008, è consultabile all'indirizzo: http://lesrapports.ladocumentationfrancaise.fr/BRP/084000238/0000.pdf.

[3] Vedi la sezione "Documentazione".

[4] Vedi la sezione "Documentazione".

[5] Vedi la sezione "Documentazione".

[6] Il testo completo della legge è consultabile al seguente indirizzo: http://www.bundesrecht.juris.de/g10_2001/index.html.

[7] Vedi la sezione "Documentazione".

[8] Il testo completo della legge è consultabile al seguente indirizzo http://www.gesetze-im-internet.de/zfdg/index.html.

[9] Il testo completo della legge è consultabile al seguente indirizzo: http://www.bundesrecht.juris.de/tkg_2004/index.html.

[10] Il testo completo è consultabile al seguente indirizzo: http://www.gesetze-im-internet.de/tk_v_2005/index.html.

[11] Vedi la sezione "Documentazione".

[12] Il testo completo della legge è consultabile al seguente indirizzo: http://bundesrecht.juris.de/krwaffkontrg/index.html

[13] Il testo integrale della legge è disponibile all'indirizzo Internet: http://www.opsi.gov.uk/acts/acts2000/20000023.htm.

[14] Tale assunto fu, in anni passati, oggetto di critiche da parte del Lord Chancellor: cfr. il Rapporto sull'applicazione dello *Human Rights Act* pubblicato il 25 luglio 2006, consultabile presso il sito Internet del *Department for Constitutional Affairs* (ora Ministero della Giustizia) all'indirizzo: http://www.dca.gov.uk/peoples-rights/human-rights/publications.htm.

[15] Un elenco completo ed aggiornato degli *Statutory Instruments* attuativi del RIPA è disponibile presso il sito Internet del Ministero dell'Interno (*Home Office*), all'indirizzo: http://security.homeoffice.gov.uk/ripa/legislation/ripa-statutory-instruments/?version=1 .
[16] Il riferimento è al *Covert Surveillance Code of Practice* (consultabile presso il sito dello *Home Office*, all'indirizzo Internet: http://security.homeoffice.gov.uk/ripa/publication-search/ripa-cop/covert-cop?version=1); al *Covert Human Intelligence Code of Practice* (http://security.homeoffice.gov.uk/ripa/publication-search/ripa-cop/human-cop), e allo *Acquisition and disclosure of communications data revised draft code of practice* (http://security.homeoffice.gov.uk/news-and-publications1/publication-search/ripa-cop/), quest'ultimo tuttora all'esame del Parlamento ed oggetto, mentre si scrive, di una consultazione pubblica promossa dallo *Home Office*. Il *consultation paper*, dal titolo *Acquisition and Disclosure of Communication Data*, è disponibile all'indirizzo: http://www.homeoffice.gov.uk/documents/cons-2006-ripa-part1/)
[17] Eccettuati alcune ipotesi particolari (relative ai reati consistenti nell'effettuare intercettazioni illegittime, oppure a violazioni della disciplina del segreto di Stato), le intercettazioni si configurano come strumento investigativo finalizzato all'acquisizione di prove, senza avere di per sé valore probatorio. La riflessione svolta sul tema dal Governo (2003) ha confermato la validità di questo approccio in considerazione sia dei soddisfacenti risultati ottenuti – avuto riguardo anche ai costi e ai benefici -, sia della sua rispondenza al modello britannico di giustizia penale. Una sintesi delle valutazioni espresse dal Governo ad esito della *Interception as evidence review* è consultabile all'indirizzo di rete:
http://security.homeoffice.gov.uk/ripa/interception/use-interception/use-interception-review/
[18] Il più recente rapporto, pubblicato nel gennaio del 2008 per l'anno 2006, è disponibile all'indirizzo Internet: http://www.mi5.gov.uk/output/Page217.html
[19] L'IPT ha assorbito le competenze dei disciolti *Interception of Communications Tribunal*, *Security Service Tribunal* ed *Intelligence Services Tribunal*.
[20] http://www.ipt-uk.com
[21] Si tratta dello *Investigatory Powers Tribunal Act* del 2000.
[22] Occorre menzionare, per completezza, gli altri organismi esistenti nel Regno Unito con competenze di controllo e di supervisione sulle attività di autorità investigative le quali possono avvalersi dell'effettuazione di intercettazioni. Oltre allo *Interception of Communications Commissioner* e al già richiamato *Tribunal*, operano infatti lo *Intelligence Services Commissioner*, con competenza sui servizi di sicurezza, e l'*Office of Surveillance Commissioner*, competente sulle operazioni di "*covert surveillance*".
[23] Il testo del codice di condotta è disponibile presso il sito dello *Home Office*, al seguente indirizzo di rete: http://security.homeoffice.gov.uk/ripa/publication-search/ripa-cop/interception-cop.
[24] Il testo del codice al quale si fa riferimento è disponibile all'indirizzo Internet: http://www.opsi.gov.uk/si/si2003/draft/5b.pdf.
[25] STS (Sentenza del Tribunal Supremo) 2093/1994, STS 246/1995 e STS 711/1996.
[26] STS 55/1996.
[27] STC (Sentenza del Tribunale Costituzionale) 37/1989 e STC 85/1994.
[28] STS 1690/2003.
[29] STC 49/1996.
[30] STC 166/1999, STC 171/1999, STC 299/2000 e STC 14/2001.
[31] STS 2249/1994.
[32] STC 171/1999 e STC 50/2000.
[33] STS 330/2003 e STS 1690/2003.
[34] STS 184/2003 in particolare.