

## Intercettazione di comunicazioni a distanza

Überwachung der Telekommunikation - §§ 100 a e segg. StPO (CPP) della RFT

17 Dicembre 2017

Armin Kapeller

- I. Norme costituzionali
- II. Normativa soprannazionale
- III. La Telekommunikationsüberwachung quale heimliche Ermittlungsmaßnahme
- IV. Presupposti per l'intercettazione di comunicazioni a distanza
- V. Tutela del Kernbereich privater Lebensgestaltung
- VI. Difensori e limiti alle intercettazioni
- VII. Durata delle intercettazioni e competenze a disporre
- VIII. Utilizzabilità – Inutilizzabilità
- IX. Telefonia mobile
- X. La normativa introdotta nel 2007 è incostituzionale?
- XI. Rigetto dell'istanza di sospensione dell'entrata in vigore di parti della legge del 2007

### I. Norme costituzionali

Il **Fernmeldegeheimnis (segreto di comunicazione a distanza)** viene definito dall'articolo 10, comma 1, della Costituzione della RFT (Grundgesetz: GG) “**unverletzlich**” (**inviolabile**) e nel comma 2 sono indicati i casi nei quali sono lecite Beschränkungen (restrizioni), che, peraltro, sono ammissibili, se supportate da una norma di legge o regolamentare, sempre che quest'ultima sia basata su una legge.

L'espressione (antiquata) Fernmeldewesen è stata sostituita, nel 1994, con quella di **Telekommunikation**, senza che vi siano state modificazioni concernenti la disciplina sostanziale.

**Libertà e segretezza delle telecomunicazioni** vanno tutelate in quanto inerenti al **Kernbereich privater Lebensgestaltung** (“nucleo” centrale della condotta della vita privata). La Corte costituzionale federale, il Bundesverfassungsgericht (BVerfGE), ha statuito che per tutte le Überwachungsmaßnahmen deve essere osservato il “Gebot der Achtung des unantastbaren Kernbereichs privater Lebensgestaltung” (109, 279).

Il diritto alla libertà di comunicazione costituisce uno dei **pilastri di ogni ordinamento democratico**; è uno degli elementi indispensabili per garantirne il “funzionamento”. Questo diritto tutela altresì - almeno indirettamente – il pluralismo.

**Le garanzie**, è risaputo, **servono per i tempi difficili e nei tempi difficili**. La perdita del diritto alla libera comunicazione, implica “ l'uscita dai confini ” della democrazia e “ l'ingresso” nel **circuito dei regimi dispotici**. Per fare scelte consapevoli, il cittadino, nelle democrazie, ha, tra l'altro, anche il dovere di informarsi, dovere, che, a sua volta, presuppone, la libertà di comunicazione (e di informazione).

Con la normativa de quo, i Costituenti hanno voluto assicurare che **Eingriffe** in die durch Articolo 10 GG geschützte Rechtsposition der Vertraulichkeit des Wortes, sono ammissibili e leciti **soltanto in casi ben determinati e con modalita'**, anch'esse, previste in base ad una **norma di legge o regolamentare**.

L'odierno articolo 10 GG, che è stato concepito come “**einheitliches Grundrecht**”, trova il suo precedente (storico) nell'articolo 117 della Costituzione di Weimar. Il Grundrecht (diritto fondamentale) previsto dall'articolo 10 GG, **garantisce la Vertraulichkeit individueller bzw. nichtöffentlicher Kommunikation**, nei casi in cui, a causa della distanza (locale) tra gli “interlocutori”, essi devono, necessariamente, servirsi di “terzi” (ved. BVerfGE 85, 386/396 e 106, 28/36). Il diritto fondamentale de quo è stato definito dalla Corte cost. feder., kurz und bündig, come “**private Fernkommunikation**” (115, 166/182). Le garanzie contemplate nel cit. articolo consentono altresì (ved. BVerfGE 110, 33/35) la freie Entfaltung der Persönlichkeit durch einen privaten, vor der Öffentlichkeit verborgenen Austausch von Kommunikation (il libero sviluppo della personalità attraverso uno **scambio “riservato” di comunicazioni**). La “protezione” accordata dall'articolo 10 GG garantisce non soltanto la sfera privata, ma, almeno indirettamente, anche la **dignità della persona** (BVerfGE 113, 348/391). Per questo è stato detto che l'articolo 10 GG va letto e interpretato con riferimento – anche – al disposto degli articoli 1, comma 1, e 2, comma 1, GG.

Una società organizzata **vive di comunicazioni** tra le persone e tra le istituzioni. I **mezzi di comunicazione**, in specie quelli moderni, hanno **inciso notevolmente** sulla circolazione del sapere, sulle abitudini di vita, sui rapporti tra cittadino e poteri pubblici. **La menzogna**, che è una specie di abuso della parola, è stata un **fattore particolarmente potente** nella storia dell'umanità. Lo è tuttora, anche se in misura minore. È stato detto che **nella fase storica**, l'uomo padroneggiava l'informazione, mentre **nell'epoca attuale**, progresso, benessere, vita pubblica e privata dipendono, in gran parte, dalla comunicazione e dall'informazione.

L'articolo 10 GG contiene un c. d. **Abwehrrecht**, vale a dire è stato concepito fondamentalmente quale difesa contro “interventi” delle autorità statali, ma altresì a tutela di “intrusioni” da parte di privati nella sfera privata dell'individuo. È stato lo stesso Bundesverfassungsgerichtshof ad affermare che il cit. **articolo 10 GG**, “besitzt einen **hohen Rang**” (67, 157/171). A proposito del diritto (fondamentale) sancito dal Fernmeldegeheimnis, è da rilevare che i **progressi tecnologici** in materia di telecomunicazioni sono stati, negli ultimi anni, veramente enormi, sia per quanto riguarda le **modalità e la velocità di trasmissione** di voci, immagini ecc., sia per quanto concerne la “conservazione”, lo “storaggio” delle stesse, la loro elaborazione nonché il loro utilizzo.

Va osservato, infine, per quanto concerne la disciplina dell'Überwachung und Aufzeichnung der Telekommunikation da parte di organi dello Stato, come previste dai §§ 100 a, 100 b, 100 g StPO, che la **normativa ha carattere tassativo** (ved. BGHSt = Corte suprema federale –sez. pen. - 31, 269; 31, 304, 306) per quanto riguarda i presupposti di ammissibilità delle intercettazioni, le modalità, gli organi competenti a disporle e a effettuarle.

## **II. Normativa soprannazionale**

La tutela della segretezza delle telecomunicazioni, inteso, questo concetto, in senso lato, è stata oggetto anche di **norme soprannazionali**, entrate in vigore posteriormente al Grundgesetz della RFT (1949).

Il diritto di ogni persona alla propria “corrispondenza” è stato sancito dall'**articolo 8, comma 1, CEDU** (firmata a Roma il 4.11.1950 e ratificata anche dalla RFT). Ha statuito la Corte europea dei diritti dell'uomo (C.edu), che questa garanzia **include** pure il diritto di comunicare con altre persone **senza interruzioni e senza censura**. Oggetto della protezione per effetto del suddetto articolo 8, è il **mezzo** di comunicazione e non il **contenuto** della comunicazione; quest'ultimo è tutelato, sotto il profilo della libertà

di espressione, dall'articolo 10 CEDU.

**Ogni interferenza** nel godimento del diritto alla segretezza delle telecomunicazioni, deve essere **giustificata** dall'essere finalizzata alla realizzazione d'interessi meritevoli di tutela. È stata la stessa CEDU a selezionare questi interessi, il cui elenco è tassativo.

**L'intercettazione di comunicazioni** telefoniche, di e-mails e di comunicazioni via Internet, costituisce **un'ingerenza** nel diritto al rispetto della "corrispondenza", da giustificarsi in base a parametri di legalità, di necessità, di proporzionalità e della legittimità del fine perseguito.

**Internet**, che ormai ha una grande diffusione, **consente all'utente** – a un costo assai modesto – non soltanto di leggere una notizia, ma anche di "darla", di "produrre" una notizia. Si tratta di una caratteristica che **azzerà la tradizionale differenza** tra chi comunica un'informazione e chi la riceve (con grande rapidità).

Le autorità degli Stati firmatari della – citata - Convenzione, sono **tenute a impedire la pubblicazione, sulla stampa**, di conversazioni telefoniche oggetto di intercettazione, se hanno **carattere privato** e se la pubblicazione **non** avviene in relazione ad un **procedimento penale**. Ved. Nota [1] in calce al presente articolo.

Per quanto riguarda i **rapporti tra l'articolo 8 CEDU e l'articolo 2 della stessa Convenzione**, è da rilevare che qualora in relazione agli stessi fatti, sia stata allegata la violazione degli articoli 2 e 8 CEDU, la scelta della Corte europea dei diritti dell'uomo (C.edu) comporta – generalmente – **l'assorbimento** della doglianza relativa all'articolo 8 (ved. C.edu L.C.B. c . Regno Unito dd. 9.6.1998).

Anche la **Carta dei diritti fondamentali dell'UE**, all'articolo 7, incentrato sul rispetto della vita privata e familiare, garantisce a ogni cittadino dell'UE, il diritto al rispetto della comunicazione. Quest'articolo è stato formulato in modo quasi identico rispetto all'articolo 8 CEDU, ma il suo ambito di tutela è più esteso. Il legislatore comunitario si è proposto anzitutto di **tutelare la fiducia del cittadino nella riservatezza dei mezzi di trasmissione delle comunicazioni interpersonali**; inoltre, ha voluto garantire il cittadino non soltanto da "interventi" delle autorità statali, ma accordargli altresì tutela per quanto concerne le comunicazioni a distanza con (altre) **persone private**.

**La comunicazione** è un comportamento essenziale dell'attività umana in quanto attraverso la stessa si condividono analisi, si sviluppano relazioni di fiducia tra persone, si trasmettono decisioni, si ascoltano pareri, si organizzano, se necessario, mobilitazioni. Internet fornisce **l'opportunità di esprimere** – senza limiti di tempo e di luogo – opinioni, consente di interloquire con altri soggetti acquisendo il loro parere, di rivolgersi direttamente e rapidamente alle autorità. La comunicazione attraverso i mezzi che la tecnologia odierna ci offre, è stata definita **un potere proprio della modernità**; l'accesso a questi mezzi produce una diffusione del potere e la creazione di nuovi soggetti con possibilità di determinare opinioni. Chiunque può diventare protagonista lanciando una notizia o promuovendo un raduno. Grazie ad Internet si può venire a **conoscenza – in tempo reale** – di ciò che succede in ogni parte del mondo; infatti, la "rete" **"annulla il tempo e lo spazio"**.

**Restrizioni** al diritto de quo sono ammissibili se sussistono **due presupposti fondamentali**: 1) le Beschränkungen devono essere imposte per fini attinenti all'interesse generale e, 2) con riferimento all'obiettivo proposto, non devono costituire limitazioni sproporzionate, irragionevoli o comunque tali da "intaccare" sostanzialmente l'esercizio del diritto che si vuole garantire.

L'esigenza di assicurare la **riservatezza (Vertraulichkeit) delle comunicazioni a distanza** impone agli Stati aderenti (all'UE) di emanare adeguate norme (interne) atte ad assicurare che servizi di telecomunicazione accessibili alla generalità degli abitanti, provvedano all'installazione di **congegni tecnici idonei a escludere l'Abhören, il Mithören l'Abfangen**,

**l'Überwachen l'Aufzeichnen** nonché lo “**storaggio**” von Nachrichten, se effettuato da privati o da organi dello Stato (non autorizzati). Le operazioni ora elencate, se eseguite da autorità statali, devono rispondere alle esigenze sopra esposte e possono avvenire soltanto nei **casi e con le modalità previste dalla legge**.

La Corte europea dei diritti dell'uomo (**C.edu**), più volte, ha ribadito che il diritto fondamentale alla riservatezza delle telecomunicazioni può subire restrizioni soltanto se le stesse sono appositamente previste da una norma di legge interna e se lo scopo dei relativi provvedimenti risponde ad un **pubblico interesse**; inoltre, se la loro adozione è giustificata da pressanti esigenze riconducibili alla comunità e se vi è proporzionalità tra il “mezzo” impiegato e il fine, che col provvedimento ci si prefigge (in questo senso ved. p. es. C.edu Slg 2004, I – 3025 Karner; Slg 2003, I – 5659 Schmidberger).

### **III. La Telekommunikationsüberwachung quale heimliche Ermittlungsmaßnahme**

Premesso quanto ora esposto, **vediamo in che modo sono disciplinate le intercettazioni di comunicazioni a distanza nell'ordinamento processual-penale della RFT.**

**Per Telekommunikationsüberwachung s'intende** il “procedimento” tecnico consistente nella captazione e nella registrazione di notizie di qualsiasi specie sotto forma di voce, immagini o documentale. Si tratta di una **heimlichen Ermittlungsmethode**, con la quale il legislatore della RFT ha reagito alle innovazioni tecnologiche che si erano prodotte nel settore delle telecomunicazioni e alle “Möglichkeiten” che le stesse hanno offerto anche alla criminalità in genere e a quella organizzata in particolare; ha reagito altresì alle non poche pronunzie di incostituzionalità emesse dal BVerfGE con riferimento alla disciplina ante 2007.

La Telekommunikationsüberwachung, che comprende, come già detto, altresì l'Aufzeichnung (la registrazione) e la conservazione di quanto trasmesso e ricevuto, costituisce una verdeckte, heimliche Ermittlungsmaßnahme, un **mezzo di indagine segreto, “occulto”**. Occorre, in proposito, osservare che heimliche Ermittlungsmaßnahme **non equivale a verheimlichtes Vorgehen**. Con la prima espressione s'intende soltanto un “Vorgehen, das der Wahrnehmungsfähigkeit des Beschuldigten nicht zugänglich ist” (non è percepibile da parte dell'indagato), con la precisazione, però, che si tratta di una non percepibilità “provvisoria”, cioè **esclusa, fino a quando perdurano le indagini (preliminari)**. Il “settore” delle intercettazioni di comunicazioni a distanza, è un “settore” particolarmente delicato in quanto l'Heimlichkeit der Ermittlungen o, meglio, gli heimlichen, verhaltensbeobachtenden Eingriffe (nella sfera eminentemente privata della persona) **impediscono all'indagato**, inconsapevole dell'Ermittlungsmaßnahme, **l'esercizio di diritti essenziali di difesa** (nemo se detegere tenetur). Data la delicatezza di Eingriffe del genere - il BVerfGE 129, 208 (240) ha parlato di “eingriffsintensive Ermittlungsmaßnahmen”-comportano per l'allgemeinen Persönlichkeitsrecht (ved. BVerfGE 106, 28 (39 f)) e per l'Integrität informationstechnischer Anlagen, le norme dettate in materia di Telekommunikationsüberwachung, sono di stretta interpretazione (BGH St – Corte suprema federale 31, 296 (298)) e l'ammissibilità delle intercettazioni è circoscritta, in linea di massima, alla Sachaufklärung (accertamento dei fatti) e alla Fahndung des Beschuldigten (ricerca dell'indagato).

A seguito dell'emanazione della direttiva comunitaria 2006/24/EG del 15.3.2006, il legislatore della RFT ha modificato – con il **Gesetz zur Neuregelung der Telekommunikationsüberwachung**, entrato in vigore l'1.1.2008 – in modo sostanziale la precedente disciplina in materia di intercettazione delle comunicazioni a distanza. La Corte cost. feder. (Bundesverfassungsgericht – BVerfGE) ha ritenuto che le novazioni normative di cui alla cit. legge, **non contrastino con il GG**; in particolare, i Giudici delle Leggi, non hanno ravvisato incostituzionalità nell'“elenco” (di reati, per i quali sono ammissibili le intercettazioni di comunicazioni a distanza) di cui al comma 2° del § 100 a StPO (CPP); si veda in proposito BVerfGE

Per quanto concerne la c.d. **lückenlose Rundumüberwachung della persona**, effettuata con l'impiego - cumulativo - di intercettazioni e di altre verdeckte Ermittlungsmaßnahmen, la stessa è stata dichiarata inammissibile (unzulässig) dalla Corte cost. feder. (ved. BVerfGE 109, 279, 323) e dal BGH St 54, 69, 102 ff).

#### **IV. Presupposti per l'intercettazione di comunicazioni a distanza**

**Presupposto indispensabile per una Telekommunikationsüberwachungsmaßnahme** è, anzitutto, un **provvedimento (Anordnung)**, dato per iscritto, dal giudice ed emesso previa richiesta del PM. Qualora vi sia pericolo nel ritardo, è competente pure il PM ad emettere l'Anordnung, nel qual caso, però, entro tre giorni, deve avvenire, a pena di decadenza, la gerichtliche Bestätigung (la conferma o, meglio, la convalida da parte del giudice). **L'Anordnung, che ha validità (massima) di tre mesi**, è prorogabile di ulteriori tre mesi, qualora, tenuto conto dei risultati delle indagini espletate, persistano i presupposti per la Maßnahme. La parte dispositiva dell'Anordnung deve contenere, oltre alla menzione del reato, per il quale si procede, i **motivi dell'indispensabilità (Unentbehrlichkeit)** del ricorso all'intercettazione (ved. BGH St 47, 362), le indicazioni di cui al § 100 b, comma 2, StPO (generalità, residenza/domicilio dell'indagato, numero dell'apparecchio sottoposto a controllo, termine finale delle operazioni di captazione).

Si ha **inutilizzabilità dei risultati** delle intercettazioni, se manca la richterliche Anordnung (BGH St 31, 308 f e 35, 32) oppure se non vi è neppure il sospetto che sia stata commessa una delle Katalogstraftaten (di cui al § 100 a StPO).

L'intercettazione e la registrazione delle telecomunicazioni è ammissibile soltanto se sussiste un c. d. **Anfangsverdacht (sospetto "iniziale")** circa la commissione di uno dei **reati** ("Katalogtaten") indicati tassativamente nel **§ 100 a, comma 2, della StPO**. L'Anfangsverdacht deve essere desumibile da fatti certi (bestimmte Tatsachen); in questo senso ved. BVerfGE 113, 348 (385). Il sospetto non deve, quindi, essere, ne' hinreichend, ne' dringend. **Le Katalogstraftaten** erano originariamente soltanto delitti contro lo Stato e altri **reati di particolare gravità (Schwerstdelikte)**. Con il passar del tempo, il "Katalog" è stato notevolmente ampliato, anche se va osservato che a seguito di una sentenza pronunciata dalla Corte cost. feder., il legislatore ha inserito (nel comma 1, n. 2, del § 100 a StPO) l'inciso che la Katalogstraftat deve essere **"auch im Einzelfall schwerwiegend"**.

Il fatto, per il quale viene disposta l'intercettazione, deve dunque auch im Einzelfall schwer wiegen, vale a dire, deve essere, nel caso concreto, **von erheblicher Bedeutung (di rilevante gravità)**. Quest'ultimo requisito è stato introdotto dal legislatore a seguito della sentenza del BVerfGE 107, 299 (322). Ai fini della valutazione della sussistenza, o meno, della rilevante gravità, il giudice deve fare **riferimento ai criteri previsti per la determinazione della pena**.

**Altro presupposto indispensabile** affinché possa essere disposta la Telekommunikationsüberwachung, è che le indagini o l'accertamento dei fatti oppure del luogo, nel quale si ritiene che si trovi l'indagato, **sarebbero impossibili o notevolmente difficoltosi senza il ricorso a intercettazione delle telecomunicazioni**. È stato detto che l'Überwachung des Fernmeldeverkehrs – in osservanza al Verhältnismäßigkeitsprinzip (principio di proporzionalità) – ha, **in linea di principio, carattere sussidiario (ist subsidiär)**.

Il comma 4 del § 100 a StPO prevede poi una c. d. **negative Voraussetzung** nel senso che non devono sussistere Anhaltspunkte per ritenere che l'intercettazione venga chiesta al solo **fine di acquisire notizie inerenti al Kernbereich privater Lebensgestaltung della persona** da sottoporre a intercettazione; si parla in proposito di Kernbereichsschutz.

## **V. Tutela del Kernbereich privater Lebensgestaltung**

Qualora, nel corso di intercettazioni, ritualmente disposte, **emergano fatti attinenti al Kernbereich privater Lebensgestaltung** e se gli stessi sono stati **registrati** (cosa, che può senz'altro succedere nel caso in cui la Telekommunikationsüberwachung è automatizzata), queste **registrazioni sono inutilizzabili** (sind unverwendbar) e devono essere **immediatamente cancellate o comunque ogni documentazione delle stesse deve essere distrutta**; dell'avvenuta cancellazione/distruzione deve essere dato atto in un apposito verbale. Si parla in proposito di kombiniertem Beweisthemaverbot und Verwertungsverbot. Si vede che il legislatore ha avuto **fiducia negli inquirenti**, ai quali spetta di cancellare le registrazioni inutilizzabili e di effettuare la distruzione dei documenti che sono unverwertbar.

Il provvedimento, col quale vengono ordinate intercettazioni di telecomunicazioni, può essere disposto inizialmente **soltanto nei confronti dell'indagato**. Può tuttavia riguardare anche altre persone, c.d. Zielpersonen, qualora, sulla base di fatti certi, sia da ritenere che le stesse "passino", cioè **consegnino**, all'indagato, notizie, in realtà dirette a quest'ultimo oppure **inoltrino**, utilizzando i loro mezzi di telecomunicazione (fungendo quindi da Nachrichtenmittler), **notizie dell'indagato**.

## **VI. Difensori e limitazioni alle intercettazioni**

L'intercettazione delle telecomunicazioni dei Nachrichtenmittler è lecita, anche se si tratta di persone che hanno il **diritto di astenersi dal deporre** ex § 52 StPO. Per quanto concerne l'Überwachung der Telekommunikation di persone vincolate al **segreto professionale**, trova applicazione il § 160 a StPO, anch'esso introdotto dalla legge federale del dicembre 2007, di cui si è parlato sopra.

Le telecomunicazioni dei **difensori non** possono essere **sottoposte a intercettazione**, ostandovi il disposto del § 148 StPO (ved. BGH St 33, 347 (349)); neppure, se il difensore stesso è sospettato quale concorrente (del cliente) nel reato, per il quale si procede, a meno che non sia (già) stato disposto l'**Ausschluss des Verteidigers vom Verfahren** (ai sensi del § 138 a, 1° c., n. 1, StPO), vale a dire, se al difensore è stata inibita la "partecipazione" al procedimento nel senso che non può difendere il cliente neppure in procedimenti diversi da quello, nel quale wurde der Ausschluss verfügt.

Qualora venga **intercettato un colloquio o una comunicazione per iscritto, tra difensore e cliente** in violazione del § 148 StPO e se nel corso di tale comunicazione dallo stesso emergono indizi di reità in ordine al **reato di Strafvereitelung** (§ 258 a StGB=CP), le risultanze di queste intercettazioni **non sono utilizzabili** nei confronti del difensore. Infatti, un'applicazione in via analogica del § 97, comma 2, StPO (che consente il sequestro presso il difensore) non è ammissibile (ved. BGH St 33, 347).

Per quanto concerne il **materiale probatorio emerso** durante una Telekommunikationsüberwachung, ritualmente disposta, esso è **utilizzabile dagli organi di polizia ai fini della Gefahrenabwehr** (ai sensi del § 477 StPO), se il pericolo inerisce alla sicurezza pubblica.

Unverwertbares Material non è utilizzabile, in sede dibattimentale, quale prova (BGH St 26, 298), ne' può essere utilizzato a fini di contestazione (BGH St 27, 355).

## **VII. Durata delle intercettazioni e competenze a disporle**

Il provvedimento giudiziale, mediante il quale è stata **ordinata l'intercettazione, non può essere disposto per un periodo di tempo eccedente la durata di tre mesi**

, ma è prorogabile. Il termine trimestrale inizia a decorrere dalla data del provvedimento d'intercettazione e non dal giorno d'inizio delle operazioni di intercettazione (ved. BGH St 44, 243).

**Competente per l'esecuzione delle operazioni di intercettazione è il PM** (§ 36, 2° c., StPO) che comunica al dirigente della società di telecomunicazioni il provvedimento giudiziale, per iscritto o, anche oralmente, se vi è urgenza (in Eilfällen). La Staatsanwaltschaft trasmette la suddetta **Anordnung anche alla polizia che predispone materialmente la messa in opera dei congegni elettronici necessari per la "captazione"**. Soltanto il giudice, il PM e gli organi di polizia, ai quali sono "affidate" le indagini, possono **prendere cognizione del contenuto delle comunicazioni intercettate**. Non risulta, almeno finora, che contenuti di intercettazioni di comunicazioni a distanza siano stati – **abusivamente** (vale a dire al di fuori dei casi in cui la pubblicazione era attinente ad un procedimento penale) – **"passati" alla stampa** e quindi pubblicati.

Prevede il § 100 b, comma 4, StPO che le operazioni di intercettazione devono **cessare immediatamente**, se vengono a mancare i presupposti legittimanti l'effettuazione delle stesse e tutto il **"materiale" non necessario o non più necessario** ai fini del procedimento, nel quale le intercettazioni sono state disposte, deve **immediatamente essere distrutto**. Chi è stato sottoposto a intercettazione, deve essere **notiziato**, dopo la conclusione delle relative operazioni, cioè delle intercettazioni avvenute ad insaputa del "controllato".

**L'Überwachungsmaßnahme di cui al § 100 a StPO è comprensiva di tutte le trasmissioni e captazioni di notizie, suoni, voci, documenti ecc.;** con inclusione, pertanto, anche di dati ed e-mails che si trovano ancora presso il provider. Se, invece, i dati sono già presso il destinatario, possono essere oggetto di sequestro (probatorio) ex § 94 StPO.

### **VIII. Utilizzabilità - Inutilizzabilità**

Se nel corso delle intercettazioni di telecomunicazioni gli inquirenti – **casualmente - vengono a conoscenza di un fatto costituente reato** che si ritiene **commesso** non dall'indagato, ma **da altra persona** (c.d. Zufallserkenntnisse), **l'utilizzabilità** (§ 477, 2° c., StPO) **non è esclusa**, se si tratta di uno dei reati elencati nel § 100 a StPO (Katalogtat). Se durante un'intercettazione, ritualmente disposta, per l'accertamento di uno dei reati indicati nel cit. § 100 a StPO, gli inquirenti vengono a **conoscenza di un reato non facente parte delle c.d. Katalogstraftaten**, le prove acquisite relativamente a questa "Nichtkatalogtat" sono inutilizzabili. Se invece si tratta di **altra Katalogtat** (vale a dire, di un reato diverso da quello, per il quale è stata emanata l'Anordnung auf Telekommunikationsüberwachung, ma che figura nell'elenco previsto dal § 100 a StPO), il materiale probatorio acquisito è **utilizzabile ai fini della prova di questo reato** (ved. BGH St 32, 10). I risultati delle intercettazioni possono però essere utilizzati ai fini della **prova di Nichtkatalogtaten, se queste ultime "stehen mit der Katalogtat in engem Zusammenhang"** (BGHSt 26, 298, 302 e 28, 122, 125ff.). Gli inquirenti possono comunque "trarre spunto" da Zufallsfunde per iniziare un nuovo procedimento penale per il (nuovo) reato emerso (BGH St 27, 355). Parimenti utilizzabili sono Abhörungsergebnisse, se riguardano la commissione di uno dei reati p. e p. dai § 129 e segg. StGB (CP); in questo senso ved. ord.ze BGH St 28, 122 e 54, 69, 79 f.

**Non costituisce violazione del Fernmeldegeheimnis (segreto di telecomunicazione)**, se l'abbonato **consente** – spontaneamente e volontariamente – ad un agente della polizia di assistere alla comunicazione, senza che il destinatario della stessa sia stato previamente informato del **Mithören (ascolto)**; in questo senso ved. BGH St 39, 335 (339f) e 42, 139 (154).

Per quanto concerne le **modalità**, attraverso le quali le risultanze delle intercettazioni vengono **acquisite agli atti del procedimento**, la StPO tace. In proposito è però "venuto in soccorso" il BGH,

statuendo (27, 135) che può procedersi, o **all'ascolto dell'intera registrazione sonora del colloquio** oppure **alla "zu den Aktannahme" della trascrizione integrale della registrazione** (ciò avviene "im Wege des Urkundenbeweises", mediante **acquisizione di documentazione agli atti del processo**).

Il **divieto di utilizzabilità** è nella **disponibilità dell'imputato** (ist für den Angeklagten disponibel), per cui il giudice del dibattimento non può utilizzare le prove ottenute attraverso le intercettazioni ai fini della decisione, soltanto se l'imputato **non si è opposto** – tempestivamente – **all'utilizzabilità** delle stesse.

## **IX. Telefonia mobile**

**Se vi è sospetto**, suffragato da fatti certi, che una **persona, titolare e utilizzatrice di un telefono mobile**, abbia commesso un reato o abbia concorso nella perpetrazione di una Straftat von erheblicher Bedeutung (di rilevante gravità), è ammissibile, ai fini dell'**accertamento del reato nonché del luogo in cui si trova l'indagato**, l'individuazione del relativo apparecchio, del numero della scheda e della località, in cui l'abbonato si trova. A tal fine vengono impiegati i c.d. IMSI-chatchers. Anche questa Maßnahme deve essere **disposta dal giudice** (vi è Richtervorbehalt); se vi sono motivi di urgenza, sussiste l'**Eilkompetenz del PM**. Il provvedimento del giudice ha **validità di 6 mesi** ed il termine è prorogabile di altri 6 mesi. Anche nel caso de quo, l'**Eingriff è ammissibile soltanto se il ricorso a "mezzi" meno "invasivi" si prospetta nicht zielführend**. Le misure de quo possono essere disposte pure in caso di **tentativo** di uno dei reati di cui sopra oppure se vi è stata Vorbereitung (atti preparatori) di un reato che rientra tra le Katalogtaten. Notizie che si riferiscono a terzi, possono essere acquisite se, per motivi tecnici, il loro rilievo non può essere evitato.

## **X. La normativa introdotta nel 2007 è incostituzionale?**

La **disciplina delle intercettazioni**, come prevista, – innovativamente a seguito dell'emanazione della legge federale del dicembre 2007 (entrata in vigore l'1.1.2008) concernente la Neuregelung der Telekommunikationsüberwachung und anderer, verdeckter Ermittlungsmaßnahmen – dall'attuale § 100 a StPO, **non è andata esente da critiche**, specie per quanto riguarda la **costituzionalità** della neo-normativa.

### **A**

In particolare, è stata affermata l'**incostituzionalità** del § 100 a, commi 2 e 4, StPO, ma la Corte cost. feder., con Beschluss (ordinanza) dd. 12.10.2011, ha **rigettato le dedotte censure**, ritenendo la Verfassungsmäßigkeit (conformità alla Costituzione) delle suddette norme di legge nonché del § 160 a StPO, anch'esso introdotto per effetto della legge federale sopra citata.

Con **Verfassungsklage**, i ricorrenti avevano **sostenuto che l'ampliamento del "catalogo" dei reati contemplati nel § 100 a, comma 2, StPO** (cioè dei reati, per il cui accertamento sono lecite le intercettazioni di telecomunicazioni a distanza), **violerebbe il principio della Verhältnismäßigkeit**. Ha però osservato il BVerfGE che la Schwere dei reati deve essere valutata non soltanto con riferimento alla pena edittale massima (di almeno 5 anni di reclusione). Per effetto dell'ampliamento delle Katalogstraftaten, sono compresi **reati che, in erheblicher Weise (in modo rilevante) influiscono sulla Funktionsfähigkeit des Staates** (sulla capacità di "funzionamento" dello Stato), delle sue istituzioni nonché sui beni giuridici – meritevoli di tutela – di privati. Rimarcavano, i giudici del Bundesverfassungsgerichtshof, che il principio della **Verhältnismäßigkeit è rispettato**, dato che tra i presupposti per l'Anordnung auf Telekommunikationsüberwachung, **figura pure che la "jeweilige Tat muss auch im Einzelfall schwer wiegen"**.

Con riferimento alla censura, secondo la quale la disciplina del § 100 a StPO, **violerebbe la dignità della persona**,



qual è prevista dall'articolo 1, comma 1, GG, il BVerfGE ha osservato che il **Kernbereich privater Lebensgestaltung non viene “intaccato”** per effetto del disposto del § 100 a StPO (bleibt unberührt). Ciò in quanto con la legge sopra citata, è stato modificato non soltanto il § 100 a StPO, ma è stato anche **introdotto, nella StPO, un nuovo paragrafo**, il 160 a, in materia di astensione dall'obbligo di deporre da parte di determinate categorie di persone. Informazioni concernenti il Kernbereich privater Lebensführung **non** possono essere **acquisite**, ne' possono essere **utilizzate** in sede di decisione (della sentenza), ne' essere utilizzate in altro modo.

Di quest'esigenza, ha affermato la Corte cost. feder., il legislatore, in occasione della redazione del § 100 a StPO, avrebbe adeguatamente tenuto conto, **inibendo anche una “zielgerichtete Erhebung kernbereichsrrelevanter Daten” e proibendo le intercettazioni** nelle quali è prevedibile, p. es., sulla base della qualità dell'interlocutore, che la notizia abbia **attinenza al suddetto Kernbereich**.

## **B**

Nel caso in cui, nel corso di intercettazioni, venissero **registrate informazioni relative al** citato Kernbereich, il comma 4 del § 100 a StPO, obbliga gli inquirenti **a cancellare immediatamente** quanto captato.

I ricorrenti avevano dedotto anche un **altro profilo di incostituzionalità**, nel senso che il § 100 a StPO non garantirebbe il diritto a un'effettiva **tutela giudiziaria**, come previsto dall'articolo 19, comma 4, GG. A ciò i giudici del BVerfGE hanno obiettato che la persona, nei cui confronti è stata disposta una verdeckte, strafprozessuale Ermittlungsmaßnahme, **deve** – sia pure ex post – **essere informata** del provvedimento adottato nei suoi confronti. **Eccezioni** al principio sancito dall'articolo 19, comma 4, GG sono, ad avviso del BVerfGE, **giustificate**, se ben circoscritte e se si tiene conto dei diritti (garantiti dalla Costituzione federale) di terzi (come p. es. nel caso in cui il provvedimento adottato (ad insaputa dell'intercettato), **non potrebbe raggiungere il fine**, se, notiziando l'intercettato, potrebbe essere messo in pericolo la vita o l'incolumità di una persona oppure se il provvedimento provocherebbe una **violazione ancora più grave** di un diritto fondamentale. A questi “postulati”, ha affermato il BVerfGE, rispondono sia il comma 2 sia il comma 4 del § 101 StPO.

A proposito del Beweiserhebungs- und Beweisverwendungsverbot, quale “normato“ nel § 160 a StPO, è stato rilevato dai giudici di Karlsruhe, che è ben vero che esso **va circoscritto a casi eccezionali**. Ciò, però, appare ammissibile nel caso de quo in considerazione dell'**obbligo dello Stato**, sancito dalla Costituzione federale, di **assicurare un'effettiva tutela penale**. I divieti di cui sopra appaiono giustificati nei casi in cui viene **“intaccata” la “Menschenwürde, die keiner Abwägung zugänglich ist” (la dignità della persona non suscettibile di bilanciamento** e che deve, quindi, in ogni caso, essere salvaguardata), se la comunicazione (come avviene p. es. in occasione di colloqui con ministri di culto o con difensori) ha per oggetto l'“unantastbaren Bereich privater Lebensgestaltung”.

Con ordinanza dd. 6.7.16, il **BVerfGE non ha ritenuto incostituzionale** una “längerfristige Überwachung des gesamten Internetverkehrs des Beschuldigten” (una prolungata intercettazione di tutto il “traffico” Internet a carico di un indagato).

Hanno fatto riferimento, in proposito, i giudici di Karlsruhe, all'**interpretazione estensiva del concetto di telecomunicazione** di cui al § 100 a StPO, nel senso di comprendervi l'invio, la trasmissione e la ricezione di notizie. Doveva, quindi, essere compresa l'intercettazione di **Internet** mediante il c. d. surfing, l'inserimento di Suchbegriffe e l'accesso a pagine del web.

I Giudici delle Leggi hanno osservato, che **in sede di interpretazione** del concetto di telecomunicazione,

deve tenersi **conto anche del Persönlichkeitsschutz**. La tutela della Vertraulichkeit riguarda non tanto - o non tanto - coloro che partecipano alla comunicazione, quanto il “**procedimento**” di trasmissione (della notizia) e l’**integrità del mezzo** a tal fine impiegato.

C

**Infondata**, secondo il BVerfGE, è l’**asserita incostituzionalità** del § 100 a StPO con riferimento alla dedotta **violazione del Bestimmtheitsgebot (principio di determinatezza)** e del **Verhältnismäßigkeitsgebot (principio di proporzionalità)**. La formulazione del § 100 a StPO non può essere, fondatamente, censurata in quanto le **garanzie** previste a tutela del Kernbereich privater Lebensgestaltung, sono **sufficienti**, sia per quanto concerne la fase di acquisizione delle prove, che quella di valutazione delle medesime.

**L’intercettazione di tutte le comunicazioni via Internet di un indagato**, anche se protratta per un notevole periodo di tempo, non possono dirsi in contrasto con i dettami della Costituzione federale, qualora venga, in ogni caso, rispettato il principio di proporzionalità e se l’Überwachungsmaßnahme è giustificata con riferimento alla **gravità del fatto**, per il quale si procede ad intercettazione e alla **gravità del sospetto** nei confronti dell’indagato.

#### **XI. Rigetto dell’istanza di sospensione dell’entrata in vigore di parti della legge del 2007**

Con ordinanza dd. 15.10. 2008, la Corte cost. feder. aveva anche **rigettato l’istanza di sospensione dell’entrata in vigore** dei commi 2 e 4 del “nuovo” paragrafo 100 a StPO (nonché della c.d. Vorratsdatenspeicherung). Aveva ritenuto il Bundesverfassungsgericht che, in base ad un **bilanciamento** tra i vantaggi che deriverebbero dalla sospensione e quelli che si produrrebbero a seguito della mancata sospensione, questi ultimi dovessero essere **ritenuti prevalenti**. La problematica doveva comunque essere oggetto di una “umfassenden Prüfung im Hauptverfahren” (di un approfondito esame nel merito). Si richiamavano, i giudici di Karlsruhe, a proposito delle doglianze concernenti il § 104, comma 2 e 4, StPO, a **precedenti decisioni**, nelle quali erano state messe in risalto: 1) le esigenze (definite “unabweisbar”) di un’**efficiente giustizia penale**, 2) l’**interesse pubblico**, in uno Stato di diritto, all’**accertamento della verità** quanto più compiutamente possibile e 3) l’importanza dell’**accertamento di reati gravi**.

L’accoglimento dell’istanza di sospensione avrebbe avuto per conseguenza che un rilevante numero di indagini per reati gravi, non avrebbe potuto nemmeno essere iniziato.

Conclusivamente appare lecita l’affermazione che la **disciplina** – in materia di intercettazione di comunicazioni a distanza, come sopra esposta e tenuto conto degli “interventi” della Corte cost. feder. – **assicura** alle persone residenti nella RFT “**einen Bereich privater Lebensführung, der der Einwirkung öffentlicher Gewalt in größtmöglichem Maße entzogen ist**”.

Mi sia consentito di citare, alla fine di quest’articolo, **una famosa frase di John Locke (1634-1704)**. “È obbligo dello Stato, garantire e tutelare la libertà di tutti; non è nei poteri dello Stato, violare i diritti individuali. Oltre alla garanzia della vita, della libertà e della proprietà, è di particolare importanza la tutela delle modalità prescelte da ciascuno per condurre la propria vita”.

Nota [1] Emblematica, appare, in proposito, la sentenza della C.edu dd. 17.7.2003 (ricorso n. 25.337/94 – Caso Craxi contro Italia (n. 1)).

Aveva ritenuto, la C.edu, che era stato violato l’articolo 8 della CEDU (diritto al rispetto della vita privata) in quanto lo Stato italiano non aveva assicurato la custodia dei verbali delle conversazioni telefoniche

intercettate, ne' poi condotto un'indagine effettiva sulla "maniera" i cui queste comunicazioni private erano state rese pubbliche dalla stampa. Inoltre, le autorità italiane non avevano rispettato le procedure legali, prima della lettura dei verbali delle conversazioni telefoniche intercettate, nel senso che avrebbero potuto escludere i passaggi delle conversazioni intercettate "prive di rapporto con la procedura" (vale dire, con le indagini per il reato di corruzione). Questa condanna era avvenuta ad unanimità dei giudici della C.edu, mentre quella per la mancata custodia dei verbali, aveva registrato una sola "dissenting opinion". La violazione dell'articolo 8 CEDU era dunque avvenuta sotto un duplice profilo e la sentenza era stata emanata dopo ca. 9 anni, quando il ricorrente ormai era deceduto e dopo che gli eredi avevano proseguito il procedimento. A titolo di "danni morali", in favore degli eredi, era stato liquidato l'importo di 2000 Euro a ciascuno di essi.

**TAG:** *Carta dei diritti fondamentali UE, intercettazioni, Intercettazioni telefoniche, RFT, Diritto dell'Unione Europea, diritto penale europeo, Diritto Tedesco*

---

### **Avvertenza**

*La pubblicazione di contributi, approfondimenti, articoli e in genere di tutte le opere dottrinarie e di commento (ivi comprese le news) presenti su Filodiritto è stata concessa (e richiesta) dai rispettivi autori, titolari di tutti i diritti morali e patrimoniali ai sensi della legge sul diritto d'autore e sui diritti connessi (Legge 633/1941). La riproduzione ed ogni altra forma di diffusione al pubblico delle predette opere (anche in parte), in difetto di autorizzazione dell'autore, è punita a norma degli articoli 171, 171-bis, 171-ter, 174-bis e 174-ter della menzionata Legge 633/1941. È consentito scaricare, prendere visione, estrarre copia o stampare i documenti pubblicati su Filodiritto nella sezione Dottrina per ragioni esclusivamente personali, a scopo informativo-culturale e non commerciale, esclusa ogni modifica o alterazione. Sono parimenti consentite le citazioni a titolo di cronaca, studio, critica o recensione, purché accompagnate dal nome dell'autore dell'articolo e dall'indicazione della fonte, ad esempio: Luca Martini, La discrezionalità del sanitario nella qualificazione di reato perseguibile d'ufficio ai fini dell'obbligo di referto ex. art 365 cod. pen., in "Filodiritto" (<https://www.filodiritto.com>), con relativo collegamento ipertestuale. Se l'autore non è altrimenti indicato i diritti sono di Inforomatica S.r.l. e la riproduzione è vietata senza il consenso esplicito della stessa. È sempre gradita la comunicazione del testo, telematico o cartaceo, ove è avvenuta la citazione.*

---