ALMA MATER STUDIORUM – UNIVERSITA' DI BOLOGNA
DIPARTIMENTO DI SCIENZE GIURIDICHE
CIRSFID

PERQUISIZIONI ON LINE INTERCETTAZIONI TELEMATICHE DATA RETENTION

Avv. Antonio Gammarota, Ph.D.
Professore a contratto, modulo "Profili giuridici dell'informatica forense"

CIRSFID
Dipartimento di Scienze Giuridiche
Alma Mater Studiorum – Università di Bologna

antonio.gammarota@unibo.it
avvocato@gammarota.it

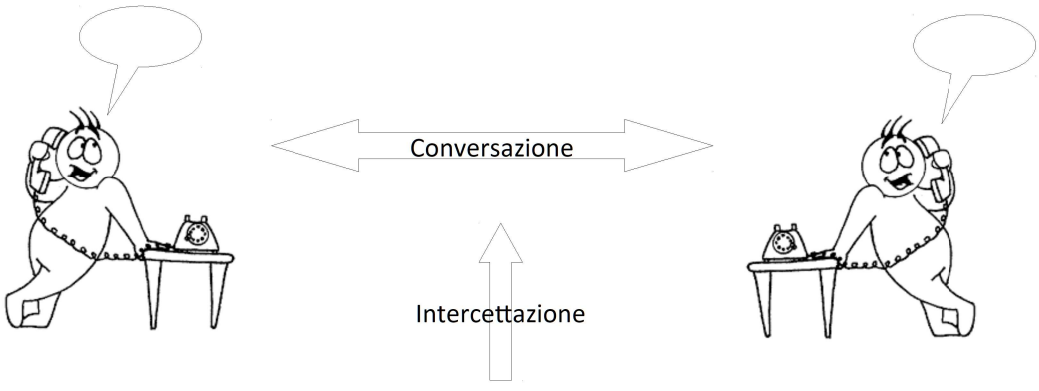
Fonti

- Libertà di espressione (art. 21, c. 1) Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali
- Inviolabilità delle comunicazioni (art. 15 Costituzione)
- Intercettazioni (artt. 266 e ss. C.p.p.)
  - di conversazioni o comunicazioni telefoniche e di altre forme di comunicazione (c.d. telefoniche) art. 266, 1 c., c.p.p.
  - comunicazioni tra presenti (c.d. ambientali) art. 266, 2 c., c.p.p.
    - nei luoghi dell'art. 615 c.p., (domicilio) se vi si sta svolgendo l'attività criminosa art. 266, 2 c., 2 p., c.p.p.
  - flussi telematici (c.d. informatiche) art. 266 bis cp.p.

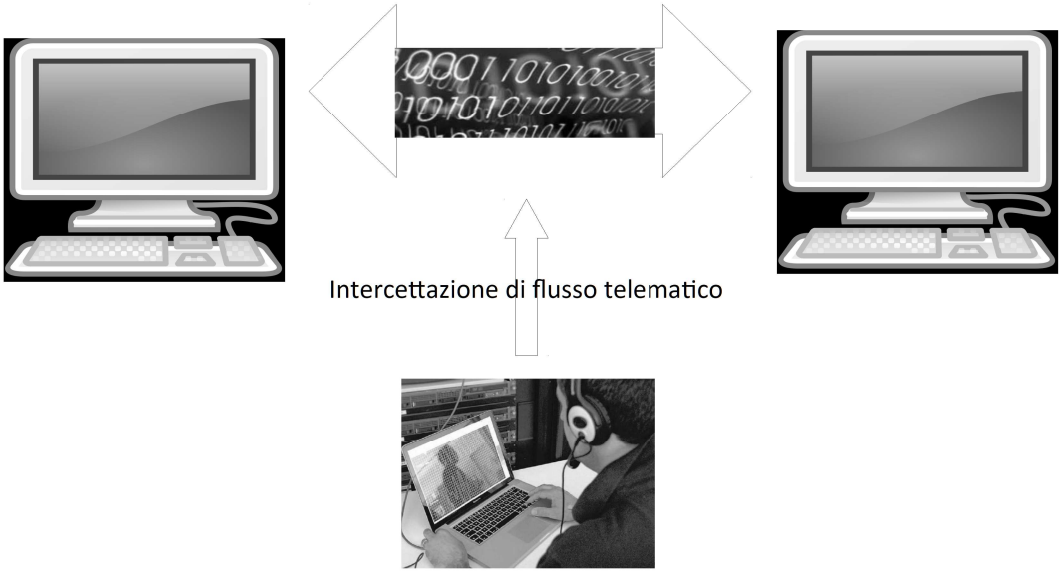
- Argomenti correlati
  - Documenti conseguenti ad intercettazioni illegali (L. 20 novembre 2006, n. 281)
  - Data retention (art. 132 D.Lgs. 196/2003)
  - art. 3 del D.Lgs. 109/08
  - c.d. "Legge Pisanu" (L. 31 luglio 2005, n. 155)
  - D. Lgs. 30 maggio 2008, n. 109

Intercettazioni di flussi telematici

Intercettazioni di comunicazioni informatiche o telematiche

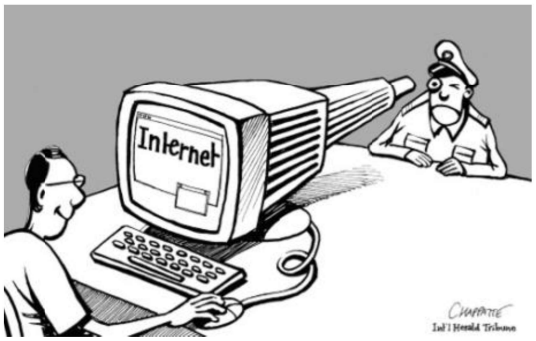


Intercettazioni di comunicazioni informatiche o telematiche



Intercettazioni di comunicazioni informatiche o telematiche

Ispezione/ Perquisizione on line (o da remoto)



Intercettazioni di comunicazioni informatiche o telematiche

Intercettazione ambientale OLD STYLE

Intercettazioni di comunicazioni informatiche o telematiche

Intercettazioni di comunicazioni informatiche o telematiche

Intercettazioni di comunicazioni informatiche o telematiche

schermatura anti intercettazione tempest sale riunioni uffici, l

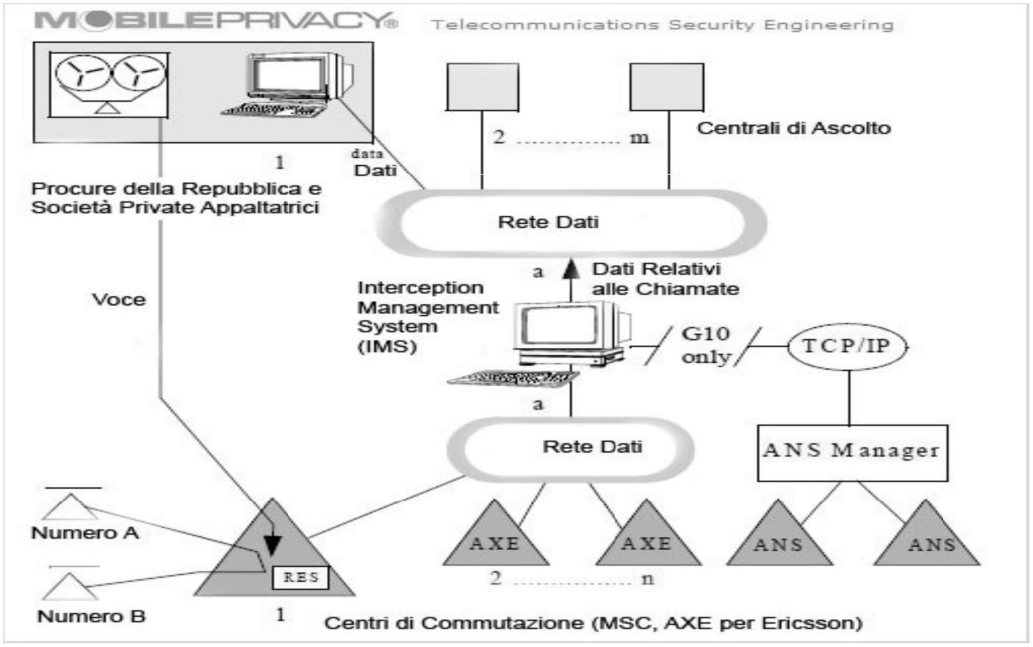
schermatura anti intercettazione tempest

[redacted] *Le stanze, locali, uffici con schermatura anti intercettazione ambientale (tempest) e telefonica consentono di proteggere l'ufficio, stanze, locali da* [redacted]

La schermatura anti intercettazione ambientale (tempest) di stanze, locali, uffici viene realizzata in locali già esistenti mediante l'immissione di pannelli appositi con all'interno la schermatura anti intercettazioni, oppure mediante la messa in opera di teli anti intercettazione che lavorano a schermatura elettromagnetica (tempest). Al posto dei vetri saranno installati degli speciali pannelli di vetro fibra trasparente con integrata una superficie di schermatura anti intercettazione. Con questi accorgimenti schermatura anti intercettazione (tempest) si ottiene su frequenze fino a 1,5 Giga hertz una inibizione dell'ordine

tenda struttura tempest anti intercettazioni

Intercettazioni di comunicazioni informatiche o telematiche



Intercettazioni di comunicazioni informatiche o telematiche

FONTI

- *art. 21, c. 1, Libertà di espressione Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali - Ogni persona ha (...) libertà di ricevere o di comunicare informazioni o idee senza che vi possa essere ingerenza da parte delle autorità pubbliche e senza considerazione di frontiera*

- *Art. 15 Cost. -* ***La libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione sono inviolabili.***

  La loro limitazione può avvenire soltanto per atto motivato dell'Autorità giudiziaria con le garanzie stabilite dalla legge.

- ***266 bis c.p.p.*** *(L. 547/93)* ***- Intercettazioni di comunicazioni informatiche o telematiche***

DISCIPLINA PER LE INTERCETTAZIONI DI COMUNICAZIONI INFORMATICHE O TELEMATICHE

- *Art. 15 Cost. - La libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione sono inviolabili.*

  La loro limitazione può avvenire ***soltanto per atto motivato dell'Autorità giudiziaria con le garanzie stabilite dalla legge.***

- *L. 547/93 →* ***266 bis c.p.p.***

- *La disciplina richiamata sarebbe quella del 267 e ss. c.p.p., ma l'art. 267 non è richiamato; mancherebbe la necessità dei presupposti e forme del provvedimento ?*

- *Dottrina (Parodi), ritiene applicabile il 267 al 266 bis c.p.p., altrimenti, il 267 c.p.p. sarebbe costituzionalmente illegittimo nella parte in cui non prevede il richiamo al 266 bis c.p.p.;*

Intercettazioni di comunicazioni informatiche o telematiche

266 c.p.p. (Limiti di ammissibilità)

1. L'**intercettazione di conversazioni o comunicazioni telefoniche e di altre forme di telecomunicazione** è consentita nei procedimenti relativi ai seguenti reati (15 Cost.):

a) delitti non colposi per i quali è prevista la pena dell'ergastolo o della reclusione superiore nel massimo a cinque anni determinata a norma dell'art. 4;

b) delitti contro la pubblica amministrazione per i quali è prevista la pena della reclusione non inferiore nel massimo a cinque anni determinata a norma dell'art. 4;

c) delitti concernenti sostanze stupefacenti o psicotrope;

d) delitti concernenti le armi e le sostanze esplosive;

e) delitti di contrabbando;

f) reati di ingiuria, minaccia, usura, abusiva attività finanziaria, (3) molestia o disturbo alle persone col mezzo del telefono.

f bis) delitti previsti dall'articolo 600 ter, terzo comma, del codice penale (4).

f-ter) delitti previsti dagli articoli 444, 473, 474, 515, 516 e 517 quater del codice penale (4);

f-quater) delitto previsto dall'articolo 612 bis del codice penale (5).

2 Negli stessi casi è consentita l'**intercettazione di comunicazioni tra presenti**. Tuttavia, qualora queste avvengano nei luoghi indicati dall'art. 614 del codice penale, l'intercettazione è consentita solo se vi è fondato motivo di ritenere che ivi si stia svolgendo l'attività criminosa (1035) (5).

Intercettazioni di comunicazioni informatiche o telematiche

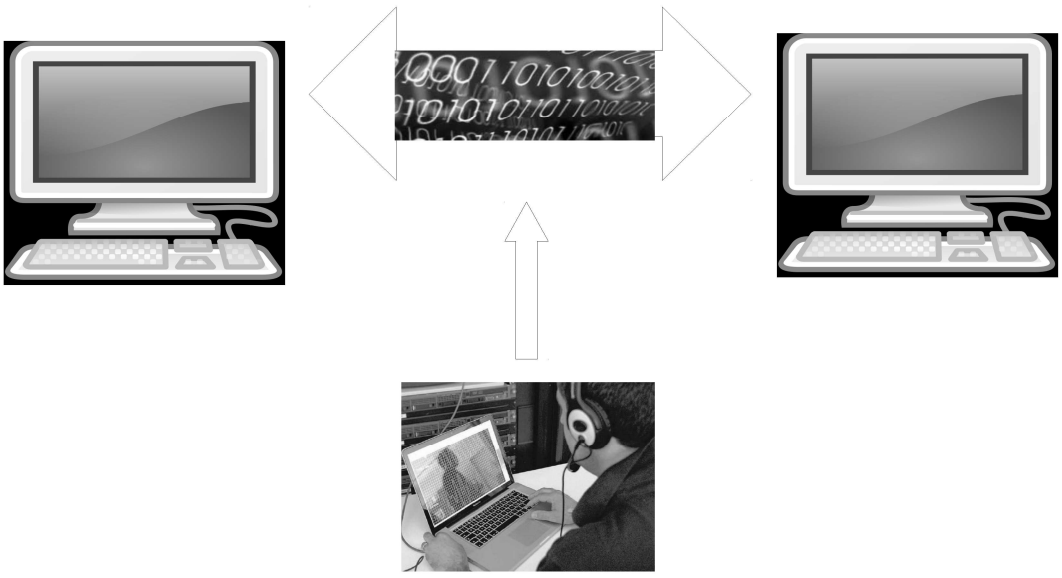
Art. 266 bis c.p.p. (Intercettazioni di comunicazioni informatiche o telematiche)

Nei procedimenti relativi ai reati indicati nell'articolo **266**, nonché **a quelli commessi mediante l'impiego di tecnologie informatiche o telematiche**, è consentita l'**intercettazione del flusso di comunicazioni relativo a sistemi informatici o telematici** ovvero **intercorrente tra più sistemi**.

Art. 267 c.p.p. (Presupposti e forme del provvedimento)
Art. 268 c.p.p. (Esecuzione delle operazioni)
Art. 269 c.p.p. (Conservazione della documentazione)
Art. 270 c.p.p. (Utilizzazione in altri procedimenti)
Art. 271 c.p.p. (Divieti di utilizzazione)

PER LE TECNICHE DI INTERCETTAZIONE SI RINVIA ALLA NETWORK FORENSICS

Intercettazioni di comunicazioni informatiche o telematiche



Intercettazioni di comunicazioni informatiche o telematiche

art. 266 c.p.p.	266 bis c.p.p.

• intercettazioni di:
  • conversazioni o comunicazioni telefoniche e di altre forme di telecomunicazione
	• intercettazione di
	  • flusso di comunicazioni relativo a:
	  • sistemi informatici o telematici ovvero
	  • intercorrente tra più sistemi

• definizione tassativa	• definizione non tassativa

• consentite per elenco tassativo di reati:
  • previsto dall'art. 266 c.p.p.
	• consentite per elenco di reati non tassativo:
	  • reati indicati nell'articolo 266
	  • reati commessi mediante l'impiego di tecnologie informatiche o telematiche

• tassatività delle garanzie e procedure richiamate dall'art. 267 c.p.p.	• garanzie e procedure non richiamate nemmeno *per relationem* dall'art. 267 c.p.p.

Intercettazioni di comunicazioni informatiche o telematiche

Questioni giuridiche

- nel 266 bis c.p.p. caduta delle garanzie costituzionali
- nel 266 bis c.p.p. ampliamento dei casi di applicabilità dell'art. 266 c.p.p.
- violazione della riserva di legge prevista dall'art. 15 Cost.
- atipicità della definizione di sistema telematico e
- (per richiamo), ampliamento dei casi dell'art. 266 bis c.p.p. Intercettazione di comunicazioni informatiche o telematiche

Questioni tecniche

- problemi tecnici relativi all'intercettazione di nuove forme di comunicazioni
  - comunicazione e scambio mediante VOIP (Voice Over Internet Protocol)
  - comunicazioni mediante canali VPN (Virtual Private Network)
  - scambio di file cifrati o steganografati

Per la giurisprudenza non sono intercettazioni telematiche

- perquisizioni on line
- acquisizioni di posta elettronica
- acquisizione dei metadati delle conversazioni digitali
- pedinamento telematico (o virtuale)
  - tracking satellitare mediante GPS (Cass. pen., Sez. V, 10 marzo 2010 (c.c. 15 gennaio 2010), n. 9667

Reati contro la inviolabilità del domicilio

- 615 bis c.p. Interferenze illecite nella vita privata
- 615 ter c.p. Accesso abusivo a sistema informatico e telematico

Reati contro la inviolabilità dei segreti

- 617 c.p. Intercettazione abusiva

DISCIPLINA PER LE INTERCETTAZIONI
DI COMUNICAZIONI INFORMATICHE O TELEMATICHE

Art. 267 c.p.p.

- **reati ex art. 266 c.p.**

- **presupposti procedura ordinaria**
  - gravi indizi di reato
  - assoluta indispensabilità per la prosecuzione delle indagini

- **procedura**
  - richiesta del PM al GIP di autorizzazione a disporre l'intercettazione
  - GIP verifica i presupposti e autorizza / non autorizza l'intercettazione

Intercettazioni di comunicazioni informatiche o telematiche

DISCIPLINA PER LE INTERCETTAZIONI
DI COMUNICAZIONI INFORMATICHE O TELEMATICHE

Art. 267 c.p.p.

- **presupposti procedura d'urgenza**
  - urgenza
  - fondato motivo di ritenere che dal **ritardo** possa derivare un **grave pregiudizio alle indagini**

- **procedura**
  - decreto motivato che dispone l'intercettazione e fissa
    - modalità delle operazioni
    - durata delle operazioni
      - non superiore a 15 giorni prorogabili con decreto motivato per periodi successivi di 15 giorni
      - permanendo i presupposti
  - comunicazione immediatamente al GIP e non oltre 24 ore
  - il GIP decide la convalida con decreto motivato entro 48 ore dal decreto
  - se il GIP non convalida il decreto entro il termine:
    - l'intercettazione non può essere proseguita
    - i risultati non possono essere utilizzati

DISCIPLINA PER LE INTERCETTAZIONI
DI COMUNICAZIONI INFORMATICHE O TELEMATICHE

Art. 267 c.p.p.

- **esecuzione**
  - PM personalmente
  - avvalendosi di un ufficiale PG
- registro riservato tenuto nell'ufficio del PM sono annotati in ordine cronologico
  - decreti che dispongono, autorizzano convalidano, prorogano le intercettazioni
  - inizio e termine delle operazioni di ciascuna intercettazione

- **esecuzione operazioni art. 268 c.p.p.**

- **conservazione della documentazione art. 269 c.p.p.**

Intercettazioni di comunicazioni informatiche o telematiche

LE NUOVE FORME DI TELECONTROLLO

- **KEYLOGGER**
- **PEDINATORE INFORMATICO**
  - **GPS**
- **CAPTATORI INFORMATICI**
  - **trojan**

- http://e-privacy.winstonsmith.org/

Intercettazioni di comunicazioni informatiche o telematiche

CAPTATORI INFORMATICI

- cosa sono: **programma spia di dispositivi digitali** (pc, tablet, smatphone)
- come funzionano: **vengono installati da remoto con un trojan**
- cosa possono fare: **TUTTO**
  - sfuggire all'antivirus
  - prendere il controllo della macchina
  - frugare nei file di log, anche di navigazione, posta elettronica, ogni altro file
  - salvare, cancellare, modificare e inviare in remoto file contenuti nella memoria
  - attivare microfono e webcam per teleascoltare e videoriprendere
  - spedire in remoto i file audio e video
  - cancellare le tracce di funzionamento
  - autodistruggersi

- v. http://e-privacy.winstonsmith.org/

Intercettazioni di comunicazioni informatiche o telematiche

IL CASO "HACKING TEAM"

da https://it.wikipedia.org/wiki/Hacking_Team

i c.d. "Trojan di Stato"

- in quanto società a partecipazione pubblica ?
- in quanto società fornitrice di trojan allo Stato ?

Cosa possono fare i software di HT ?

- Raccolta segreta di email, SMS, cronologia telefonica e relative liste di contatti
- Intercettazione di tastiere
- Spiare la cronologia delle ricerche web e catturare schermate
- Registrare telefonate
- Usare i telefoni per intercettazioni ambientali
- Mettere in funzione la foto-videocamera di telefoni o computer
- Sfruttare i sistemi GPS per geolocalizzare i soggetti sorvegliati.

CAPTATORI INFORMATICI

Sez. 5, Sentenza n. 16556 del 14/10/2009 Ud. (dep. 29/04/2010)

"È legittimo il decreto del pubblico ministero di acquisizione in copia, attraverso l'installazione di un captatore informatico, della ***documentazione informatica memorizzata nel "personal computer"*** *in uso all'imputato e installato presso un ufficio pubblico, qualora il provvedimento abbia riguardato l'estrapolazione di dati, non aventi ad oggetto un flusso di comunicazioni, già formati e contenuti nella memoria del "personal computer" o che in futuro sarebbero stati memorizzati. (Nel caso di specie, l'attività autorizzata dal P.M., consistente nel prelevare e copiare documenti memorizzati sull'"hard disk" del computer in uso all'imputato, aveva avuto ad oggetto non un "flusso di comunicazioni", richiedente un dialogo con altri soggetti, ma "una relazione operativa tra microprocessore e video del sistema elet - tronico", ossia "un flusso unidirezionale di dati" confinati all'interno dei circuiti del computer; la S.C. ha ritenuto corretta la qualificazione dell'attività di captazione in questione quale prova atipica, sottratta alla disciplina prescritta dagli artt. 266 ss. cod. proc. pen.).*

CASO MUSUMECI

CASSAZIONE VI SEZ. PENALE N. 27100/15

- **Intercettazione ambientale è lecita ex art. 266, 2 c., cpp e 15 Cost. se il luogo è**:
  - circoscritto
  - specificato ab origine
  - non ovunque si trovi il soggetto
- **Intercettazione ambientale CON CAPTATORE INFORMATICO è contraria ad art. 266, 2 c., cpp e 15 Cost. perchè il luogo è**:
  - non circoscritto
  - non specificato o addirittura assente
  - ovunque si trovi il soggetto (ubiquitario)
  - captazioni illegittime e inutilizzabili
- **Videoregistrazioni** in luoghi pubblici o aperti o esposti al pubblico:
  - non in procedimento penale → documenti (Cass. SU 26795/2006, Prisco)
  - effettuate da PG, anche d'iniziativa, → prove atipiche ex art. 189 cpp
    - salvo VR in ambito domiciliare o lesive della riservatezza (se non con provvedimento motivato dell'AG)

Intercettazioni di comunicazioni informatiche o telematiche

CASO SCURATO

CASSAZIONE, VI SEZ. PENALE, ord. 6 aprile 2016 n. 13884 rimessione alle SSUU

- va ricompreso tra le intercettazioni ambientali (captazione occulta e contestuale tra due o più soggetti attuata da un terzo estraneo mediante uno strumento di tecnico di percezione in grado di vanificare le cautele poste a protezione del carat - tere riservato di tali comunicazioni)
- il captatore per sua natura non consente di indicare e anticipatamente i luoghi interessati

- essendo il captatore informatico itinerante, va verificato se:
  - viola l'unica cautela: captazione in abitazioni o luoghi privati (solo se vi è fondato motivo di ritenere che vi si stia svolgendo l'attività criminosa)
  - controllo successivo dei risultati della captazione
  - la disciplina sulle intercettazioni consente di prescindere dall'indicazione dei luoghi

Intercettazioni di comunicazioni informatiche o telematiche

DAL DISEGNO DI LEGGE DI RIFORMA DEL CPP

LE INTERCETTAZIONI

82. Il Governo è delegato ad adottare decreti legislativi per la riforma della disciplina in materia di intercettazione di conversazioni o comunicazioni e di giudizi di impugnazione nel processo penale nonché per la riforma dell'ordinamento penitenziario, secondo i princìpi e criteri direttivi previsti dai commi 84 e 85.

84. Nell'esercizio della delega di cui al comma 82, i decreti legislativi recanti modifiche alla disciplina del processo penale, per i profili di seguito indicati, sono adottati nel rispetto dei seguenti princìpi e criteri direttivi:

a) prevedere disposizioni dirette a garantire la riservatezza delle comunicazioni, in particolare dei difensori nei colloqui con l'assistito, **e delle conversazioni telefoniche e telematiche oggetto di intercettazione, in conformità all'articolo 15 della Costituzione, attraverso prescrizioni che incidano anche sulle modalità di utilizzazione cautelare dei risultati delle captazioni e che diano una precisa scansione procedimentale per la selezione di materiale intercettativo nel rispetto del contraddittorio tra le parti e fatte salve le esigenze di indagine, avendo speciale riguardo alla tutela della riservatezza delle comunicazioni e delle conversazioni delle persone occasionalmente coinvolte nel procedimento, e delle comunicazioni comunque non rilevanti a fini di giustizia penale**, disponendo in particolare, fermi restando i limiti e i criteri di utilizzabilità vigenti, che:

(...)

DAL DISEGNO DI LEGGE DI RIFORMA DEL CPP

LE INTERCETTAZIONI

82. Il Governo è delegato ad adottare decreti legislativi per la riforma della disciplina in materia di intercettazione di conversazioni o comunicazioni e di giudizi di impugnazione nel processo penale nonché per la riforma dell'ordinamento penitenziario, secondo i princìpi e criteri direttivi previsti dai commi 84 e 85.

84. (…) 1) ai fini della selezione del materiale da inviare al giudice a sostegno della richiesta di misura cautelare, il pubblico ministero, oltre che per necessità di prosecuzione delle indagini, assicuri la riservatezza anche degli atti contenenti registrazioni di conversazioni o comunicazioni informatiche o telematiche inutilizzabili a qualunque titolo ovvero contenenti dati sensibili ai sensi dell'articolo 4, comma 1, lettera d), del codice di cui al decreto legislativo 30 giugno 2003, n. 196, che non siano pertinenti all'accertamento delle responsabilità per i reati per cui si procede o per altri reati emersi nello stesso procedimento o nel corso delle indagini, ovvero irrilevanti ai fini delle indagini in quanto riguardanti esclusivamente fatti o circostanze ad esse estranei;

2) gli atti di cui al numero 1) non allegati a sostegno della richiesta di misura cautelare siano custoditi in apposito archivio riservato, con facoltà di esame e ascolto ma non di copia, da parte dei difensori delle parti e del giudice, fino al momento di conclusione della procedura di cui all'articolo 268, commi 6 e 7, del codice di procedura penale, con il quale soltanto viene meno il divieto di cui al comma 1 dell'articolo 114 del medesimo codice relativamente agli atti acquisiti; prevedere la semplificazione delle condizioni per l'impiego delle intercettazioni delle conversazioni e delle comunicazioni telefoniche e telematiche nei procedimenti per i più gravi reati dei pubblici ufficiali contro la pubblica amministrazione;

Intercettazioni di comunicazioni informatiche o telematiche

DAL DISEGNO DI LEGGE DI RIFORMA DEL CPP

LE INTERCETTAZIONI

82. Il Governo è delegato ad adottare decreti legislativi per la riforma della disciplina in materia di intercettazione di conversazioni o comunicazioni e di giudizi di impugnazione nel processo penale nonché per la riforma dell'ordinamento penitenziario, secondo i princìpi e criteri direttivi previsti dai commi 84 e 85.

84. (…) e) disciplinare le intercettazioni di comunicazioni o conversazioni tra presenti mediante immissione di captatori informatici in dispositivi elettronici portatili, prevedendo che:

1) l'attivazione del microfono avvenga solo in conseguenza di apposito comando inviato da remoto e non con il solo inserimento del captatore informatico, nel rispetto dei limiti stabiliti nel decreto autorizzativo del giudice;

2) la registrazione audio venga avviata dalla polizia giudiziaria o dal personale incaricato ai sensi dell'articolo 348, comma 4, del codice di procedura penale, su indicazione della polizia giudiziaria operante che è tenuta a indicare l'ora di inizio e fine della registrazione, secondo circostanze da attestare nel verbale descrittivo delle modalità di effettuazione delle operazioni di cui all'articolo 268 del medesimo codice;

3) l'attivazione del dispositivo sia sempre ammessa nel caso in cui si proceda per i delitti di cui all'articolo 51, commi 3- bis e 3-quater, del codice di procedura pe-nale e, fuori da tali casi, nei luoghi di cui all'articolo 614 del codice penale soltanto qualora ivi si stia svolgendo l'attività criminosa, nel rispetto dei requisiti di cui all'articolo 266, comma 1, del codice di procedura penale; in ogni caso il decreto autorizzativo del giudice deve indicare le ragioni per le quali tale specifica modalità di intercettazione sia necessaria per lo svolgimento delle indagini;

DAL DISEGNO DI LEGGE DI RIFORMA DEL CPP

LE INTERCETTAZIONI

82. Il Governo è delegato ad adottare decreti legislativi per la riforma della disciplina in materia di intercettazione di conversazioni o comunicazioni e di giudizi di impugnazione nel processo penale nonché per la riforma dell'ordinamento penitenziario, secondo i princìpi e criteri direttivi previsti dai commi 84 e 85.

84. (…) 4) il trasferimento delle registrazioni sia effettuato soltanto verso il server della Procura così da garantire originalità e integrità delle registrazioni; al termine della registrazione il captatore informatico venga disattivato e reso definitivamente inutilizzabile su indicazione del personale di polizia giudiziaria operante;

5) siano utilizzati soltanto programmi informatici conformi a requisiti tecnici stabiliti con [redacted] da emanare entro trenta giorni dalla data di entrata in vigore dei decreti legislativi di cui al presente comma, che tenga costantemente conto dell'evoluzione tecnica al fine di garantire che tali programmi si limitino ad effettuare le operazioni espressamente disposte secondo standard idonei di affidabilità tecnica, di sicurezza e di efficacia;

6) fermi restando i poteri del giudice nei casi ordinari, ove ricorrano concreti casi di urgenza, il pubblico ministero possa disporre le intercettazioni di cui alla presente lettera, limitatamente ai delitti di cui all'articolo 51, commi 3-bis e 3-quater, del codice di procedura penale, con successiva convalida del giudice entro il termine massimo di quarantotto ore, sempre che il decreto d'urgenza dia conto delle specifiche situazioni di fatto che rendono impossibile la richiesta al giudice e delle ragioni per le quali tale specifica modalità di intercettazione sia necessaria per lo svolgimento delle indagini;

(...)

Intercettazioni di comunicazioni informatiche o telematiche

DAL DISEGNO DI LEGGE DI RIFORMA DEL CPP

LE INTERCETTAZIONI

82. Il Governo è delegato ad adottare decreti legislativi per la riforma della disciplina in materia di intercettazione di conversazioni o comunicazioni e di giudizi di impugnazione nel processo penale nonché per la riforma dell'ordinamento penitenziario, secondo i princìpi e criteri direttivi previsti dai commi 84 e 85.

84. (…) 7) i risultati intercettativi così ottenuti possano essere utilizzati a fini di prova soltanto dei reati oggetto del provvedimento autorizzativo e possano essere utilizzati in procedimenti diversi a condizione che siano indispensabili per l'accertamento dei delitti di cui all'articolo 380 del codice di procedura penale;

8) non possano essere in alcun modo conoscibili, divulgabili e pubblicabili i risultati di intercettazioni che abbiano coinvolto occasionalmente soggetti estranei ai fatti per cui si procede;

DAL DISEGNO DI LEGGE DI RIFORMA DEL CPP

LE INTERCETTAZIONI

82. Il Governo è delegato ad adottare decreti legislativi per la riforma della disciplina in materia di intercettazione di conversazioni o comunicazioni e di giudizi di impugnazione nel processo penale nonché per la riforma dell'ordinamento penitenziario, secondo i principi e criteri direttivi previsti dai commi 84 e 85.

84. (…) i) prevedere la legittimazione dell'imputato ad appellare avverso la sentenza di condanna, nonché avverso la sentenza di proscioglimento emessa al termine del dibattimento salvo che sia pronunciata con le formule: «il fatto non sussiste» o «l'imputato non ha commesso il fatto»;

l) escludere l'appellabilità delle sentenze di condanna alla sola pena dell'ammenda e delle sentenze di proscioglimento o di non luogo a procedere relative a contravvenzioni punite con la sola pena dell'ammenda o con una pena alternativa;

m) prevedere la titolarità dell'appello incidentale in capo all'imputato e limiti di proponibilità.

Intercettazioni di comunicazioni informatiche o telematiche

DAL DISEGNO DI LEGGE DI RIFORMA DEL CPP

LE INTERCETTAZIONI

82. Il Governo è delegato ad adottare decreti legislativi per la riforma della disciplina in materia di intercettazione di conversazioni o comunicazioni e di giudizi di impugnazione nel processo penale nonché per la riforma dell'ordinamento penitenziario, secondo i principi e criteri direttivi previsti dai commi 84 e 85.

84. (…) f) prevedere la ricorribilità per cassazione soltanto per violazione di legge delle sentenze emesse in grado di appello nei procedimenti per i reati di competenza del giudice di pace;

g) prevedere che il procuratore generale presso la corte di appello possa appellare soltanto nei casi di avocazione e di acquiescenza del pubblico ministero presso il giudice di primo grado;

h) prevedere la legittimazione del pubblico ministero ad appellare avverso la sentenza di proscioglimento, nonché avverso la sentenza di condanna solo quando abbia modificato il titolo del reato o abbia escluso la sussistenza di una circostanza aggravante ad effetto speciale o abbia stabilito una pena di specie diversa da quella ordinaria del reato;

i) prevedere la legittimazione dell'imputato ad appellare avverso la sentenza di condanna, nonché avverso la sentenza di proscioglimento emessa al termine del dibattimento salvo che sia pronunciata con le formule: «il fatto non sussiste» o «l'imputato non ha commesso il fatto»;

l) escludere l'appellabilità delle sentenze di condanna alla sola pena dell'ammenda e delle sentenze di proscioglimento o di non luogo a procedere relative a contravvenzioni punite con la sola pena dell'ammenda o con una pena alternativa;

m) prevedere la titolarità dell'appello incidentale in capo all'imputato e limiti di proponibilità. 85. Fermo restando quanto previsto dal-l'articolo 41-bis della legge 26 luglio 1975, n. 354, e successive modificazioni,

Intercettazioni di comunicazioni informatiche o telematiche

DAL DISEGNO DI LEGGE DI RIFORMA DEL CPP
L'ART. 360 CPP

28. All'**articolo 360 del codice di procedura penale**, dopo il comma 4 è inserito il seguente: «*4-bis. La riserva di cui al comma 4 perde efficacia e non può essere ulteriormente formulata se la richiesta di incidente probatorio non è proposta entro il termine di dieci giorni dalla formulazione della riserva stessa*».

Quale confine tra selezione e cancellazione ?

I documenti conseguenti ad intercettazioni illegali

I documenti conseguenti ad intercettazioni illegali

240. Documenti anonimi ed atti relativi ad intercettazioni illegali. (1) (2) (3) (4) (5)

1. I **documenti** che contengono dichiarazioni anonime non possono essere acquisiti né in alcun modo utilizzati, salvo che costituiscano corpo del reato o provengano comunque dall'imputato.

2. Il pubblico ministero dispone l'immediata secretazione e la custodia in luogo protetto dei **documenti, dei supporti e degli atti concernenti dati e contenuti di conversazioni o comunicazioni, relativi a traffico telefonico e telematico, illegalmente formati o acquisiti.** Allo stesso modo provvede per i documenti formati attraverso la raccolta illegale di informazioni. Di essi è vietato effettuare copia in qualunque forma e in qualunque fase del procedimento ed il loro contenuto non può essere utilizzato.

3. Il pubblico ministero, acquisiti i documenti, i supporti e gli atti di cui al comma 2, entro quarantotto ore, **chiede al giudice per le indagini preliminari di disporne la distruzione.**

(…)

Avv. Antonio Gammarota © avvocato@gammarota.it

I documenti conseguenti ad intercettazioni illegali

240. Documenti anonimi ed atti relativi ad intercettazioni illegali. (1) (2) (3) (4) (5)

(...)

4. Il giudice per le indagini preliminari entro le successive quarantotto ore fissa l'udienza da tenersi entro dieci giorni, ai sensi dell'articolo 127, dando avviso a tutte le parti interessate, che potranno nominare un difensore di fiducia, almeno tre giorni prima della data dell'udienza.

5. Sentite le parti comparse, il giudice per le indagini preliminari legge il provvedimento in udienza e, nel caso ritenga sussistenti i presupposti di cui al comma 2, **dispone la distruzione dei documenti, dei supporti e degli atti di cui al medesimo comma 2 e vi dà esecuzione subito dopo alla presenza del pubblico ministero e dei difensori delle parti**.

6. Delle operazioni di distruzione è redatto apposito verbale, nel quale si dà atto dell'avvenuta intercettazione o detenzione o acquisizione illecita dei documenti, dei supporti e degli atti di cui al comma 2 nonché delle modalità e dei mezzi usati oltre che dei soggetti interessati, senza alcun riferimento al contenuto degli stessi documenti, supporti e atti.

I documenti conseguenti ad intercettazioni illegali

240. Documenti anonimi ed atti relativi ad intercettazioni illegali. (1) (2) (3) (4) (5)

(...)

(1) Questo articolo è stato così sostituito dall'art. 1 del D.L. 22 settembre 2006, n. 259, convertito, con modificazioni, nella L. 20 novembre 2006, n. 281.

(2) Art. così sostituito ex d.l. 22-9-2006, n. 259, conv. in l. 20-11-2006, n. 281 (art. 1), in materia di intercettazioni telefoniche. Il testo previgente così disponeva: «240. Documenti anonimi. — 1. I documenti che contengono dichiarazioni anonime non possono essere acquisiti né in alcun modo utilizzati salvo che costituiscano corpo del reato o provengano comunque dall'imputato».

(3) Cfr. art. 3, d.l. 259/2006, conv. in l. 281/2006 cit., che così dispone: «3. — 1. Chiunque consapevolmente detiene gli atti, i supporti o i documenti di cui sia stata disposta la distruzione ai sensi dell'articolo 240 del codice di procedura penale è punito con la pena della reclusione da sei mesi a quattro anni.

2. Si applica la pena della reclusione da uno a cinque anni se il fatto di cui al comma 1 è commesso da un pubblico ufficiale o da un incaricato di pubblico servizio».

(4) La Corte costituzionale, con sentenza n. 173 del 22 aprile 2009, ha dichiarato l'illegittimità costituzionale di questo comma, nella parte in cui non prevede, per la disciplina del contraddittorio, l'applicazione dell'art. 401, commi 1 e 2, dello stesso codice.

(5) La Corte costituzionale, con sentenza n. 173 del 22 aprile 2009, ha dichiarato l'illegittimità costituzionale di questo comma, nella parte in cui non esclude dal divieto di fare riferimento al contenuto dei documenti, supporti e atti, nella redazione del verbale previsto dalla stessa norma, le circostanze inerenti l'attività di formazione, acquisizione e raccolta degli stessi documenti, supporti e atti.

I documenti conseguenti ad intercettazioni illegali

512. Lettura di atti per sopravvenuta impossibilità di ripetizione. (1)

1. Il giudice, a richiesta di parte, dispone che sia data lettura degli atti assunti dalla polizia giudiziaria, dal pubblico ministero, dai difensori delle parti private (2) e dal giudice nel corso dell'udienza preliminare [422] quando, per fatti o circostanze imprevedibili, ne è divenuta impossibile la ripetizione.

- 1bis. **È sempre consentita la lettura dei verbali relativi all'acquisizione ed alle operazioni di distruzione degli atti di cui all'articolo 240** (3).

(*1) Art. modificato ex d.l. 8-6-1992, n. 306, conv. in l. 7-8-1992, n. 356 (art. 8, c. 2).*

(2) Le parole: «, dai difensori delle parti private» sono state inserite ex art. 18, l. 7-12-2000, n. 397.

(3) Comma aggiunto ex art. 2, d.l. 22-9-2006, n. 259, conv. in l. 20-11-2006, n. 281 (Intercettazioni telefoniche).

Intercettazioni telematiche e dati esterni relativi al traffico telefonico e telematico

Intercettazioni e dati esterni al traffico telefonico

I c.d. "**dati esterni**" relativi al traffico telefonico" = (dati diversi dal contenuto delle comunicazioni cui fanno riferimento)

Evoluzione della disciplina dell'acquisizione

- **Teoria meno rigorosa: Cass. 7994/95**

  È da considerarsi regolare ed utilizzabile *l'allegazione al fascicolo processuale di* ***tabulati Sip****, inviati* ***senza richiesta scritta e motivata del p.m.****, attestanti telefonate intercorse tra due cellulari e, quindi,* ***solo dati esteriori di conversazioni telefoniche*** *senza alcuna conoscenza dei relativi contenuti, in quanto l'art. 234 comma 1 c.p.p., secondo cui è consentita l'acquisizione di scritti o di altri documenti che rappresentano fatti, persone, cose mediante la fotografia, la cinematografia, la fonografia o qualsiasi altro mezzo, non stabilisce formalità alcuna di acquisizione.* (Cass. pen., sez. I, 6 giugno 1995, n. 7994, Micic, Cass. pen. 1996, 2624 (s.m.), Giust. pen. 1996, III, 600 (s.m.))"

- **Teoria più rigorosa: Cass. SU 21/98**

  Per quanto i dati a genesi informatica o telematica, una volta stampati, diventassero documenti intellegibili, l'attività di **acquisizione dei tabulati** derivanti dal flusso telematico fosse **soggetta alla disciplina delle intercettazioni**.

avvocato@gammarota.it

Intercettazioni e dati esterni al traffico telefonico

I c.d. "dati esterni" relativi al traffico telefonico" = (dati diversi dal contenuto delle comunicazioni cui fanno riferimento)

Evoluzione della disciplina dell'acquisizione

- **Ma altri giudici di merito si rifacevano alla Corte costituzionale**

  Il decreto motivato dell'Autorità giudiziaria, ovvero del p.m. emesso nella fase delle indagini preliminari, deve ritenersi sufficiente **ai fini dell'acquisizione e, dunque, della utilizzabilità dei c.d. tabulati del traf - fico telefonico dei cellulari**, in ossequio al disposto dell'art. 15 cost. ed in sintonia con quanto recentemente osservato dalla C. cost. (Tribunale Perugia, 29 giugno 1999, Giacchini e altro, Rass. giur. umbra 1999, 859 nota (CONFALONIERI))

- Successivamente, sulla base di Corte Cost. 81/93 (in FI, 1993, I, 2132), **Cass., SU n. 16/00,** ritenne che ai tabulati con i dati esterni **non fossero applicabili le garanzie dell'intercettazione in quanto documenti acquisibili ex art. 256 cpp,** in un corret - to contemperamento delle esigenze della giustizia con quelle della tutela del dirit - to alla libertà e segretezza della corrispondenza ex art. 15 Cost.

avvocato@gammarota.it

Intercettazioni e dati esterni al traffico telefonico

I c.d. “dati esterni” relativi al traffico telefonico" = (dati diversi dal contenuto delle comunicazioni cui fanno riferimento)

Corte costituzionale 38/2019 (Rel. Zanon)

Non è incostituzionale la norma che impone al giudice di chiedere alla Camera di appartenenza del parlamentare l’autorizzazione a utilizzare in giudizio, come mezzi di prova, i tabulati telefonici di utenze intestate a terzi, venute in contatto con quella del parlamentare.

Il riferimento, nel terzo comma dell’articolo 68 della Costituzione, a «conversazioni o comunicazioni» induce a ritenere che siano coperti dalla garanzia costituzionale anche i dati ad esse “esteriori”, in quanto “fatti comunicativi” ricavabili da un tabulato: data e ora delle conversazioni o delle comunicazioni, durata, utenze coinvolte. Del resto, il termine «comunicazioni» ha, tra i suoi comuni significati, quello di «contatto», «rapporto», «collegamento», ed evoca proprio i dati e le notizie che un tabulato telefonico è in grado di rivelare.

Intercettazioni e dati esterni al traffico telefonico

I c.d. “dati esterni” relativi al traffico telefonico" = (dati diversi dal contenuto delle comunicazioni cui fanno riferimento)

Corte costituzionale 38/2019 (Rel. Zanon)

La questione era stata sollevata dal Gip del Tribunale di Bologna, secondo il quale il terzo comma dell’articolo 68 della Costituzione imporrebbe l’autorizzazione della Camera solo per sottoporre i membri del Parlamento a intercettazioni di conversazioni e comunicazioni, senza menzionare i tabulati. La legge ordinaria avrebbe quindi esteso illegittimamente l’ambito di applicazione della prerogativa costituzionale.

La Corte costituzionale, però, non è stata d’accordo.

Tra l’altro, la sentenza rileva che la ragion d’essere della garanzia costituzionale non è la tutela della privacy del parlamentare bensì della libertà della funzione che egli esercita, in conformità alla natura delle immunità parlamentari, dirette a proteggere l’autonomia e l’indipendenza delle Camere rispetto a indebite invadenze di altri poteri e solo strumentalmente destinate a riverberare i propri effetti in favore di chi è investito della funzione.

Intercettazioni e dati esterni al traffico telefonico

I c.d. “dati esterni” relativi al traffico telefonico" = (dati diversi dal contenuto delle comunicazioni cui fanno riferimento)

Corte costituzionale 38/2019 (Rel. Zanon)

Per queste ragioni, la garanzia si estende all’utilizzo in giudizio del tabulato telefonico, in quanto atto idoneo a incidere sulla libertà di comunicazione del parlamentare.

Conservazione dei dati di traffico (Data retention)

Le modifiche al C.P.P. a seguito della L. 48/2008

CONSERVAZIONE DEI DATI DI TRAFFICO

D.Lgs. 30 giugno 2003 n. 196

Art. 132. Conservazione di dati di traffico per altre finalità (1)(12)

1. Fermo restando quanto previsto dall'articolo 123, comma 2, **i dati relativi al traffico telefonico, sono conservati dal fornitore** per **ventiquattro mesi dalla data della comunicazione**, per finalità di accertamento e repressione dei reati, mentre, per le medesime finalità, **i dati relativi al traffico telematico**, esclusi comunque i contenuti delle comunicazioni, **sono conservati dal fornitore per dodici mesi dalla data della comunicazione**. (2)

1-*bis*. **I dati relativi alle chiamate senza risposta**, trattati temporaneamente da parte dei fornitori di servizi di comunicazione elettronica accessibili al pubblico oppure di una rete pubblica di comunicazione, sono conservati per **trenta giorni**. (3)

2. *[abrogato]* (4)

(...)

Le modifiche al C.P.P. a seguito della L. 48/2008

CONSERVAZIONE DEI DATI DI TRAFFICO

D.Lgs. 30 giugno 2003 n. 196

Art. 132. Conservazione di dati di traffico per altre finalità (1)(12)

(…)

3. Entro il termine di cui al comma 1, i dati sono acquisiti presso il fornitore con decreto motivato del pubblico ministero anche su istanza del difensore dell'imputato, della persona sottoposta alle indagini, della persona offesa e delle altre parti private.

Il difensore dell'imputato o della persona sottoposta alle indagini può richiedere, direttamente al fornitore i dati relativi alle utenze intestate al proprio assistito con le modalità indicate dall'articolo 391-quater del codice di procedura penale.

La richiesta di accesso diretto alle comunicazioni telefoniche in entrata può essere effettuata solo quando possa derivarne un pregiudizio effettivo e concreto per lo svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397; diversamente, i diritti di cui agli articoli da 12 a 22 del Regolamento possono essere esercitati con le modalità di cui all'articolo 2- undecies, comma 3, terzo, quarto e quinto periodo. (22)

(22) Comma già modificato dall'art. 6, comma 3, lett. e), del decreto legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155.

Le modifiche al C.P.P. a seguito della L. 48/2008

CONSERVAZIONE DEI DATI DI TRAFFICO

D.Lgs. 30 giugno 2003 n. 196

Art. 132. Conservazione di dati di traffico per altre finalità (1)(12)

(...)

4-*ter*. Il **Ministro dell'interno** o, su sua delega, **i responsabili degli uffici centrali specialistici in materia informatica o telematica** della **Polizia di Stato**, dell'**Arma dei carabinieri** e del **Corpo della guardia di finanza**, nonché gli altri soggetti indicati nel comma 1 dell'articolo 226 delle norme di attuazione, di coordinamento e transitorie del codice di procedura penale, di cui al decreto legislativo 28 luglio 1989, n. 271, possono ordinare, anche in relazione alle eventuali richieste avanzate da autorità investigative straniere, ai fornitori e agli operatori di servizi informatici o telematici di conservare e proteggere, secondo le modalità indicate e per un periodo non superiore a novanta giorni, i dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, ai fini dello svolgimento delle investigazioni preventive previste dal citato articolo 226 delle norme di cui al decreto legislativo n. 271 del 1989, ovvero per finalità di accertamento e repressione di specifici reati. Il provvedimento, prorogabile, per motivate esigenze, per una durata complessiva non superiore a sei mesi, può prevedere particolari modalità di custodia dei dati e l'eventuale indisponibilità dei dati stessi da parte dei fornitori e degli operatori di servizi informatici o telematici ovvero di terzi. (8)

(...)

Le modifiche al C.P.P. a seguito della L. 48/2008

CONSERVAZIONE DEI DATI DI TRAFFICO

D.Lgs. 30 giugno 2003 n. 196

Art. 132. Conservazione di dati di traffico per altre finalità (1)(12)

(...)

4-*quater*. Il fornitore o l'operatore di servizi informatici o telematici cui è rivolto l'ordine previsto dal comma 4-ter deve ottemperarvi senza ritardo, fornendo immediatamente all'autorità richiedente l'assicurazione dell'adempimento. Il fornitore o l'operatore di servizi informatici o telematici è tenuto a mantenere il segreto relativamente all'ordine ricevuto e alle attività conseguentemente svolte per il periodo indicato dall'autorità. In caso di violazione dell'obbligo si applicano, salvo che il fatto costituisca più grave reato, le disposizioni dell'articolo 326 del codice penale. (8)

4-*quinquies*. I provvedimenti adottati ai sensi del comma 4-ter sono comunicati per iscritto, senza ritardo e comunque entro quarantotto ore dalla notifica al destinatario, al pubblico ministero del luogo di esecuzione il quale, se ne ricorrono i presupposti, li convalida. In caso di mancata convalida, i provvedimenti assunti perdono efficacia. (8)

(...)

Le modifiche al C.P.P. a seguito della L. 48/2008

CONSERVAZIONE DEI DATI DI TRAFFICO

D.Lgs. 30 giugno 2003 n. 196

Art. 132. Conservazione di dati di traffico per altre finalità (1)(12)

(…)

5. Il trattamento dei dati per le finalità di cui al comma 1 è effettuato nel **rispetto delle misure e degli accorgimenti a garanzia dell'interessato prescritti dal Garante secondo le modalità di cui all'articolo 2-quinqiuesdecies**, volti a garantire che i dati conservati possiedano i medesimi requisiti di **qualità**, **sicurezza** e **protezione dei dati in rete**, nonché ad indicare le modalità tecniche per la periodica distruzione dei dati, decorsi i termini di cui al comma 1. (28)

5- bis. E' fatta salva la disciplina di cui all'articolo 24 della legge 20 novembre 2017, n. 167.

(29) 23 Comma abrogato dall´art. 2 , comma 1, lett. c), del decreto legislativo 30 maggio 2008, n. 109.

(28) Comma già modificato dall´art. 2, comma 1, lett. d), del decreto legislativo 30 maggio 2008, n. 109

Le modifiche al C.P.P. a seguito della L. 48/2008

SCHEMATIZZANDO

- **dati relativi al traffico telefonico**
  - sono conservati dal fornitore per **24 mesi** dalla data della comunicazione
    - per finalità di accertamento e repressione dei reati

- **dati relativi al traffico telematico**, esclusi comunque i contenuti delle comunicazioni,
  - sono conservati dal fornitore per **12 mesi** dalla data della comunicazione.
    - per finalità di accertamento e repressione dei reati

- **dati relativi alle chiamate senza risposta**, trattati temporaneamente da parte dei fornitori di servizi di comunicazione elettronica accessibili al pubblico oppure di una rete pubblica di comunicazione,
  - sono conservati per **30 giorni**

Le modifiche al C.P.P. a seguito della L. 48/2008

Art. 4 bis 1 c. d.l.18 febbraio 2015 n. 7 conv. in L. 17 aprile 2015 n. 43
finalità di terrorismo

- **dati relativi al traffico telefonico e telematico**
  - conservazione fino al 31 dicembre 2016 PROROGATO 31 dicembre 2017
  - per finalità di accertamento e repressione dei reati

- **dati relativi alle chiamate senza risposta**, trattati temporaneamente da parte dei fornitori di servizi di comunicazione elettronica accessibili al pubblico oppure di una rete pubblica di comunicazione
  - idem

Le modifiche al C.P.P. a seguito della L. 48/2008

SCHEMATIZZANDO

- **PM** - **decreto motivato**,
  - anche su istanza del **difensore** di
    - imputato
    - persona sottoposta alle indagini
    - persona offesa
    - altre parti private
  - dati entranti e uscenti

  - **Difensore dell'indagato o dell'imputato:**
    - dati di traffico uscente, a richiesta diretta al fornitore dei dati relativi alle utenze intestate al proprio assistito (art. 391-quater c.p.p.)
    - dati di traffico entrante, alle condizioni ex art. 8, c.2, lett. f). (5)

Le modifiche al C.P.P. a seguito della L. 48/2008

SCHEMATIZZANDO

Il **Ministro dell'interno** o, su sua delega,

- i responsabili degli uffici centrali specialistici in materia informatica o telematica della Polizia di Stato
- dell'Arma dei carabinieri
- del Corpo della guardia di finanza
- nonché gli altri soggetti indicati nel comma 1 dell'articolo 226 delle norme di attuazione, di coordinamento e transitorie del codice di procedura penale, di cui al decreto legislativo 28 luglio 1989, n. 271,
- **anche su richiesta di autorità investigative straniere**
  - **possono ordinare**
    - ai fornitori di servizi informatici o telematici
    - agli operatori di servizi informatici o telematici
  - **di conservare e proteggere, secondo le modalità indicate**
    - i dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni
    - ai fini dello svolgimento delle **investigazioni preventive** previste dal citato articolo 226 delle norme di cui al decreto legislativo n. 271 del 1989,
    - ovvero **per finalità di accertamento e repressione** di specifici reati.

Le modifiche al C.P.P. a seguito della L. 48/2008

SCHEMATIZZANDO

- durata provvedimento
  - fino a **90 giorni**
  - fino a **6 mesi,** prorogabile per motivate esigenze

- contenuto provvedimento
  - può prevedere particolari modalità di custodia dei dati
  - e l'eventuale indisponibilità dei dati stessi
    - da parte dei fornitori e degli operatori di servizi informatici o telematici
    - ovvero di terzi. (8)

Le modifiche al C.P.P. a seguito della L. 48/2008

SCHEMATIZZANDO

- **obblighi del richiedente**
  - comunicazione dell'ordine al PM del luogo di esecuzione
    - per iscritto
    - senza ritardo e comunque entro quarantotto ore dalla notifica al destinatario,

- **obblighi del PM del luogo di esecuzione**
  - verifica dei presupposti ed eventuale convalida.
  - in caso di mancata convalida, i provvedimenti assunti perdono efficacia.

- **obblighi del fornitore o l'operatore di servizi informatici o telematici ordinato**
  - deve ottemperarvi senza ritardo,
  - fornendo immediatamente all'autorità richiedente **l'assicurazione** dell'adempimento.
  - **mantenere il segreto** relativamente:
    - all'ordine ricevuto
    - alle attività conseguentemente svolte per il periodo indicato dall'autorità

Le modifiche al C.P.P. a seguito della L. 48/2008

CONSERVAZIONE DEI DATI DI TRAFFICO

Art. 4-bis del decretto legge 18 febbraio 2015, n. 7, convertito, con modificazioni, dalla legge 17 aprile 2015, n. 43

Disposizioni in materia di conservazione dei dati di traffico telefonico e telematico

1. Al fine di poter agevolare le indagini esclusivamente per i reati di cui agli articoli 51, comma 3-quater, e 407, comma 2, lettera a), del codice di procedura penale, in deroga a quanto stabilito dall'articolo 132, comma 1, del codice di cui al decreto legislativo 30 giugno 2003, n. 196, e successive modificazioni, e fermo restando quanto stabilito dall'articolo 123, comma 2, del medesimo codice, **i dati relativi al traffico telefonico effettuato a decorrere dalla data di entrata in vigore della legge di conversione del presente decreto sono conservati dal fornitore fino al 31 dicembre 2016 per finalità di accertamento e repressione dei reati**. Per le medesime finalità **i dati relativi al traffico telematico effettuato a decorrere dalla data di entrata in vigore della legge di conversione del presente decreto**, esclusi comunque i contenuti della comunicazione, **sono conservati dal fornitore fino al 31 dicembre 2016.**

2. **I dati relativi alle chiamate senza risposta**, effettuate a decorrere dalla data di entrata in vigore della legge di conversione del presente decreto, trattati temporaneamente da parte dei fornitori di servizi di comunicazione elettronica accessibile al pubblico oppure di una rete pubblica di comunicazione, **sono conservati fino al 31 dicembre 2016**.

3. Le disposizioni di cui ai commi 1 e 2 cessano di applicarsi a decorrere dal 1° gennaio 2017.

CONSERVAZIONE DEI DATI DI TRAFFICO

obblighi del richiedente

rispetto delle misure e degli accorgimenti a garanzia dell'interessato prescritti ai sensi dell'articolo 17, volti a garantire che i dati conservati possiedano i medesimi requisiti di qualità, sicurezza e protezione dei dati in rete, nonché a: (9)

a) prevedere in ogni caso specifici sistemi di autenticazione informatica e di autorizzazione degli incaricati del trattamento di cui all'allegato B);

b) [soppressa] (10)

c) [soppressa] (10)

d) indicare le modalità tecniche per la periodica distruzione dei dati, decorsi i termini di cui al comma 1. (11)

Art. 17. Trattamento che presenta rischi specifici

1. Il trattamento dei dati diversi da quelli sensibili e giudiziari che presenta rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che può determinare, è ammesso nel rispetto di misure ed accorgimenti a garanzia dell'interessato, ove prescritti.

2. Le misure e gli accorgimenti di cui al comma 1 sono prescritti dal Garante in applicazione dei principi sanciti dal presente codice, nell'ambito di una verifica preliminare all'inizio del trattamento, effettuata anche in relazione a determinate categorie di titolari o di trattamenti, anche a seguito di un interpello del titolare.

Le modifiche al C.P.P. a seguito della L. 48/2008

Corte di Giustizia UE

- **sentenza dell'8 aprile 2014 C-293/12 and C-594/12 (Digital rights Ireland) dichiara l'illegittimità della direttiva "Frattini" (2006/24/Ce) per violazione del principio di proporzionalità nel bilanciamento tra diritto alla protezione dei dati personali ed esigenze di pubblica sicurezza e annulla la direttiva 2006/24/Ce**

  I commi 1 e 1-bis dell'articolo 132 del decreto legislativo 196 del 30 giugno 2003, come introdotti dal decreto legislativo 30 maggio 2008, n. 109, costituivano attuazione della direttiva 2006/24/Ce riguardante la conservazione dei dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/Ce.

- v. anche sentenza (Grande Sezione) 21 dicembre 2016 (cause riunite C-203/15 e C-698/15).

Le modifiche al C.P.P. a seguito della L. 48/2008

GARANTE PRIVACY

"L'acquisizione dei dati stessi, inoltre, deve secondo la corte di giustizia essere soggetta a specifiche condizioni, incluso il controllo da parte di un giudice o un'autorità indipendente. La sorveglianza non può mai essere generalizzata e massiva ma, lo precisa la corte di giustizia nella recente sentenza Tele2, deve fondarsi su ***requisiti individualizzanti,*** *rivolgendosi cioè nei confronti di soggetti coinvolti, in qualche misura, in attività criminose ovvero* ***limitandosi a specifici luoghi nei quali emergano esigenze investigative relative****, sempre,* ***a gravi reati*** *e previa* ***adeguata delimitazione temporale della durata della conservazione****".*

Le modifiche al C.P.P. a seguito della L. 48/2008

DEROGA PER TERRORISMO, ANCHE INTERNAZIONALE: 72 MESI

GARANTE PRIVACY

Data Retention fino a 6 anni? Scelta del Parlamento incomprensibile'.

di Luigi Garofalo | 24 Ottobre 2017, ore 14:04

https://www.key4biz.it/data-retention-6-anni-scelta-del-parlamento-incomprensibile-videointervento-antonello-soro/203324/

LA BOCCIATURA

Garante Privacy europeo: 'Grave errore Data Retention in Italia fino a 6 anni'

di Luigi Garofalo | 26 Febbraio 2019, ore 11:10

https://www.key4biz.it/garante-privacy-europeo-grave-errore-data-retention-in-italia-fino-a-6-anni/244933/

Le modifiche al C.P.P. a seguito della L. 48/2008

DEROGA PER TERRORISMO, ANCHE INTERNAZIONALE: 72 MESI

Legge Europea 2017 c.d. DIRETTIVA ASCENSORI

L. 20.11.2017 n. 167 in G.U. S. G. n. 277 del 27.11.2017 recante **Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione europea - Legge europea 2017**

Art. 24 Termini di conservazione dei dati di traffico telefonico e telematico

In attuazione dell'**articolo 20 della direttiva (UE) 2017/541 del Parlamento europeo e del Consiglio, del 15 marzo 2017, sulla lotta contro il terrorismo e che sostituisce la decisione quadro 2002/475/GAI del Consiglio, al fine di garantire strumenti di indagine efficace in considerazione delle straordinarie esigenze di contrasto del terrorismo, anche internazionale,** per le finalità dell'accertamento e della repressione dei reati di cui agli articoli 51, comma 3-quater, e 407, comma 2, lettera a), del codice di procedura penale **il termine di conservazione dei dati di traffico telefonico e telematico nonché dei dati relativi alle chiamate senza risposta**, di cui all'articolo 4-bis, commi 1 e 2, del decreto-legge 18 febbraio 2015, n. 7, convertito, con modificazioni, dalla legge 17 aprile 2015, n. 43, è stabilito in **settantadue mesi**, in deroga a quanto previsto dall'articolo 132, commi 1 e 1-bis, del codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196.

Dati esterni da conservare ex art. 3 del D.Lgs. 109/08

Definizioni (D.Lgs. 109/08)

*a) per **utente**: qualsiasi persona fisica o giuridica che utilizza un servizio di comunicazione elettronica accessibile al pubblico, senza esservi necessariamente abbonata;*

*b) per **dati relativi al traffico**: qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione, ivi compresi i dati necessari per identificare l'abbonato o l'utente;*

*c) per **dati relativi all'ubicazione**: ogni dato trattato in una rete di comunicazione elettronica che indica la posizione geografica dell'apparecchiatura terminale dell'utente di un servizio di comunicazione elettronica accessibile al pubblico, ivi compresi quelli relativi alla cella da cui una chiamata di telefonia mobile ha origine o nella quale si conclude;*

*d) per **traffico telefonico**: le chiamate telefoniche, incluse le chiamate vocali, di messaggeria vocale, in conferenza e quelle basate sulla trasmissione dati, purchè fornite da un gestore di telefonia, i servizi supplementari, inclusi l'inoltro e il trasferimento di chiamata, la messaggeria e i servizi multimediali, inclusi i servizi di messaggeria breve, servizi mediali avanzati e servizi multimediali;*

Dati esterni da conservare ex art. 3 del D.Lgs. 109/08

Definizioni (D.Lgs. 109/08)

*e) per **chiamata senza risposta**: la connessione istituita da un servizio telefonico accessibile al pubblico, non seguita da un'effettiva comunicazione, in quanto il destinatario non ha risposto ovvero vi è stato un intervento del gestore della rete;*

*f) per **identificativo dell'utente**: l'identificativo unico assegnato a una persona al momento dell'abbonamento o dell'iscrizione presso un servizio di accesso internet o un servizio di comunicazione internet;*

*g) per **indirizzo di protocollo internet (IP) univocamente assegnato**: indirizzo di protocollo (IP) che consente l'identificazione diretta dell'abbonato o utente che effettua comunicazioni sulla rete pubblica.*

2. Ai fini del presente decreto si applicano, altresì, le ulteriori definizioni, non ricomprese nel comma 1, elencate nell'articolo 4 del decreto legislativo 30 giugno 2003, n. 196, e successive modificazioni, recante codice in materia di protezione dei dati personali, di seguito denominato: «Codice».

Dati esterni da conservare ex art. 3 del D.Lgs. 109/08

Dati esterni che devono essere conservati (D.Lgs. 109/08)

"Art. 3. Categorie di dati da conservare per gli operatori di telefonia e di comunicazione elettronica

1. Le categorie di dati da conservare per le finalità di cui all'articolo 132 del Codice sono le seguenti:

a) i dati necessari per rintracciare e identificare la fonte di una comunicazione:

1) per la telefonia di rete fissa e la telefonia mobile:

1.1 numero telefonico chiamante;

1.2 nome e indirizzo dell'abbonato o dell'utente registrato;

2) per l'accesso internet:

2.1 nome e indirizzo dell'abbonato o dell'utente registrato a cui al momento della comunicazione sono stati univocamente assegnati l'indirizzo di protocollo internet (IP), un identificativo di utente o un numero telefonico;

3) per la posta elettronica:

3.1 indirizzo IP utilizzato e indirizzo di posta elettronica ed eventuale ulteriore identificativo del mittente;

3.2 indirizzo IP e nome a dominio pienamente qualificato del mail exchanger host, nel caso della tecnologia SMTP ovvero di qualsiasi tipologia di host relativo ad una diversa tecnologia utilizzata per la trasmissione della comunicazione;

Dati esterni da conservare ex art. 3 del D.Lgs. 109/08

Dati esterni che devono essere conservati (D.Lgs. 109/08)

a) i dati necessari per rintracciare e identificare la fonte di una comunicazione:

(…)

4) per la telefonia, invio di fax, sms e mms via internet:

4.1 data e ora (GMT) della connessione e della disconnessione dell'utente del servizio utilizzato su internet ed indirizzo IP impiegato, indipendentemente dalla tecnologia e dal protocollo usato;

4.2 dati anagrafici dell'utente registrato che ha effettuato la comunicazione;

Dati esterni da conservare ex art. 3 del D.Lgs. 109/08

Dati esterni che devono essere conservati (D.Lgs. 109/08)

b) i dati necessari per rintracciare e identificare la destinazione di una comunicazione:

1) per la telefonia di rete fissa e la telefonia mobile:

1.1 numero composto, ovvero il numero o i numeri chiamati e, nei casi che comportano servizi supplementari come l'inoltro o il trasferimento di chiamata, il numero o i numeri a cui la chiamata e' trasmessa;

1.2 nome e indirizzo dell'abbonato o dell'utente registrato;

2) per la posta elettronica:

2.1 indirizzo di posta elettronica, ed eventuale ulteriore identificativo, del destinatario della comunicazione;

2.2 indirizzo IP e nome a dominio pienamente qualificato del mail exchanger host (nel caso della tecnologia SMTP), ovvero di qualsiasi tipologia di host (relativamente ad una diversa tecnologia utilizzata), che ha provveduto alla consegna del messaggio;

2.3 indirizzo IP utilizzato per la ricezione ovvero la consultazione dei messaggi di posta elettronica da parte del destinatario indipendentemente dalla tecnologia o dal protocollo utilizzato;

(…)4) per la telefonia, invio di fax, sms e mms via internet:

4.1 data e ora (GMT) della connessione e della disconnessione dell'utente del servizio utilizzato su internet ed indirizzo IP impiegato, indipendentemente dalla tecnologia e dal protocollo usato;

4.2 dati anagrafici dell'utente registrato che ha effettuato la comunicazione;

Dati esterni da conservare ex art. 3 del D.Lgs. 109/08

Dati esterni che devono essere conservati (D.Lgs. 109/08)

b) i dati necessari per rintracciare e identificare la destinazione di una comunicazione:

(…)

3) telefonia, invio di fax, sms e mms via internet:

3.1 indirizzo IP, numero telefonico ed eventuale altro identificativo dell'utente chiamato;

3.2 dati anagrafici dell'utente registrato che ha ricevuto la comunicazione;

3.3 numero o numeri a cui la chiamata e' trasmessa, nei casi di servizi supplementari come l'inoltro o il trasferimento di chiamata;

Dati esterni da conservare ex art. 3 del D.Lgs. 109/08

Dati esterni che devono essere conservati (D.Lgs. 109/08)

(…)

c) i dati necessari per determinare la data, l'ora e la durata di una comunicazione:

1) per la telefonia di rete fissa e la telefonia mobile,

1.1 data e ora dell'inizio e della fine della comunicazione;

2) per l'accesso internet:

2.1 data e ora (GMT) della connessione e della disconnessione dell'utente del servizio di accesso internet, unitamente all'indirizzo IP, dinamico o statico, univocamente assegnato dal fornitore di accesso internet a una comunicazione e l'identificativo dell'abbonato o dell'utente registrato;

3) per la posta elettronica:

3.1 data e ora (GMT) della connessione e della disconnessione dell'utente del servizio di posta elettronica su internet ed indirizzo IP utilizzato, indipendentemente dalla tecnologia e dal protocollo impiegato;

4) per la telefonia, invio di fax, sms e mms via internet:

4.1 data e ora (GMT) della connessione e della disconnessione dell'utente del servizio utilizzato su internet ed indirizzo IP impiegato, indipendentemente dalla tecnologia e dal protocollo usato;

Dati esterni da conservare ex art. 3 del D.Lgs. 109/08

Dati esterni che devono essere conservati (D.Lgs. 109/08)

(…)

d) i dati necessari per determinare il tipo di comunicazione:

1) per la telefonia di rete fissa,

il servizio telefonico utilizzato

2) per la posta elettronica internet e la telefonia internet:

il servizio internet utilizzato

Dati esterni da conservare ex art. 3 del D.Lgs. 109/08

Dati esterni che devono essere conservati (D.Lgs. 109/08)

(…)

***e) i dati necessari per determinare le attrezzature di comunicazione degli utenti o quello che si presume essere le loro attrezzature**:*

1) per la telefonia di rete fissa,

numeri telefonici chiamanti e chiamati;

2) per la telefonia mobile:

2.1 numeri telefonici chiamanti e chiamati;

2.2 International Mobile Subscriber Identity (IMSI) del chiamante;

2.3 International Mobile Equipment Identity (IMEI) del chiamante;

2.4 l'IMSI del chiamato;

2.5 l'IMEI del chiamato;

2.6 nel caso dei servizi prepagati anonimi, la data e l'ora dell'attivazione iniziale della carta e l'etichetta di ubicazione (Cell ID) dalla quale e' stata effettuata l'attivazione;

3) per l'accesso internet e telefonia, invio di fax, sms e mms via internet:

3.1 numero telefonico chiamante per l'accesso commutato (dial-up access);

3.2 digital subscriber line number (DSL) o un altro identificatore finale di chi e' all'origine della comunicazione;

Dati esterni da conservare ex art. 3 del D.Lgs. 109/08

Dati esterni che devono essere conservati (D.Lgs. 109/08)

(…)

f) i dati necessari per determinare l'ubicazione delle apparecchiature di comunicazione mobile:

1) etichetta di ubicazione (Cell ID) all'inizio della comunicazione;

2) dati per identificare l'ubicazione geografica della cella facendo riferimento alle loro etichette di ubicazione (Cell ID) nel periodo in cui vengono conservati i dati sulle comunicazioni.

Dati esterni da conservare ex art. 3 del D.Lgs. 109/08

Dati esterni che devono essere conservati (D.Lgs. 109/08)

(…)

2. Con decreto del Presidente del Consiglio dei Ministri o del Ministro delegato per la pubblica amministrazione e l'innovazione, di concerto con i Ministri per le politiche europee, dello sviluppo economico, dell'interno, della giustizia, dell'economia e delle finanze e della difesa, sentito il Garante per la protezione dei dati personali, ***possono essere specificati, ove si renda necessario anche al fine dell'adeguamento all'evoluzione tecnologica e nell'ambito delle categorie di dati di cui alle lettere da a) ad f) del comma 1, i dati da conservare****".*

Garante privacy su trattamento dei dati di traffico telefonico e telematico

Provvedimento Generale 24 luglio 2008, Recepimento normativo in tema di dati di traffico telefonico e telematico – *24 luglio 2008 (in G.U. 13 agosto 2008 n. 189), in www.garanteprivacy.it/garante/doc.jsp?ID=1538224*

Intercettazioni telematiche

vs/

Perquisizioni on line

vs/

Sequestro di corrispondenza telematica

Le modifiche al C.P.P. a seguito della L. 48/2008

SEQUESTRO DI DATI INFORMATICI DI TRAFFICO

Art. 254-bis. – (Sequestro di dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazioni). – 1. L'autorità giudiziaria, quando dispone il **sequestro, presso i fornitori di servizi informatici, telematici o di telecomunicazioni, dei dati da questi detenuti, compresi quelli di traffico o di ubicazione**, può stabilire, per esigenze legate alla regolare fornitura dei medesimi servizi, che la loro acquisizione avvenga mediante **copia** di essi **su adeguato supporto**, con una **procedura che assicuri la conformità dei dati acquisiti a quelli originali** e la loro **immodificabilità**. In questo caso è, comunque, ordinato al fornitore dei servizi di **conservare e proteggere adeguatamente i dati originali**. (1).

(1) Articolo così modificato dall'art. 8, c. 5, della L. 48/2008, recante Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità` informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno

Le modifiche al C.P.P. a seguito della L. 48/2008

COSA SI INTENDE PER:

- … **fornitori di servizi informatici, telematici o di telecomunicazioni, dei dati da questi detenuti, compresi quelli di traffico o di ubicazione …**
  - sono i c.d. dati esterni, dati di handover, GPS ?
- **… la loro acquisizione avvenga mediante copia di essi** su adeguato supporto…
  - con quali procedure tecniche di acquisizione ?
    con quali garanzie per la difesa ?

Le modifiche al C.P.P. a seguito della L. 48/2008

COSA SI INTENDE PER:

- **…con una procedura che assicuri la conformità dei dati acquisiti a quelli originali e la loro immodificabilità.**
  - quale tipo di copia ?
  - con quali tools ?
  - le copie di dati – se tra loro conformi (hash) – diventano originali;
  - differenza con "originari"
  - rilevanza del time stamping ?
  - come si assicura l'immodificabilità ?
  - con quale procedura giuridica ?
  - Ex art. 359, 360 (117 disp. att. c.p.p.), 392, 233 c.p.p., altro ?
  - con quali garanzie difensive ?

Le modifiche al C.P.P. a seguito della L. 48/2008

ALCUNE IMPLICAZIONI:

Art. 257 c.p.p. – Riesame del decreto di sequestro

- imputato – sequestratario - quella che avrebbe diritto alla restituzione
- riesame per restrizione mediante selezione dei dati ?
- quali metodi di selezione dei dati ?

Le modifiche al C.P.P. a seguito della L. 48/2008

COSA SI INTENDE PER:

- … **fornitori di servizi informatici, telematici o di telecomunicazioni, dei dati da questi detenuti, compresi quelli di traffico o di ubicazione …**
  - sono i c.d. dati esterni, dati di handover, GPS ?

- **… la loro acquisizione avvenga mediante copia di essi** su adeguato supporto…
  - con quali procedure tecniche di acquisizione ?
    con quali garanzie per la difesa ?

- **...su adeguato supporto…**
  - quando il supporto può considerarsi "adeguato" ?

L'attività della polizia giudiziaria

Attività ad iniziativa della P.G.

352. (Perquisizioni) (1). 1. Nella flagranza del reato (382) o nel caso di evasione (385 c.p.), gli ufficiali di polizia giudiziaria (57) procedono a perquisizione personale o locale (247 ss.; coord. 225) quando hanno fondato motivo di ritenere che sulla persona si trovino occultate cose o tracce pertinenti al reato che possono essere cancellate o disperse ovvero che tali cose o tracce si trovino in un determinato luogo o che ivi si trovi la persona sottoposta alle indagini o l'evaso (103, 356; att. 113; 609 c.p.).
1-bis. Nella flagranza del reato, ovvero nei casi di cui al comma 2 quando sussistono i presupposti e le altre condizioni ivi previsti, gli ufficiali di polizia giudiziaria, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione, procedono altresì alla perquisizione di sistemi informatici o telematici, ancorché protetti da misure di sicurezza, quando hanno fondato motivo di ritenere che in questi si trovino occultati dati, informazioni, programmi informatici o tracce comunque pertinenti al reato che possono essere cancellati o dispersi.
2. (…)

(1) Articolo così modificato dall'art. 9 della L. 48/2008, recante Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno

L'attività della polizia giudiziaria

Attività ad iniziativa della P.G.

352. (Perquisizioni) (1) (Continua)
2. Quando si deve procedere alla esecuzione di un'ordinanza che dispone la custodia cautelare (293) o di un ordine che dispone la carcerazione nei confronti di persona imputata o condannata (656) per uno dei delitti previsti dall'art. 380 ovvero al fermo di una persona indiziata di delitto (384), gli ufficiali di polizia giudiziaria possono altresì procedere a perquisizione personale o locale se ricorrono i presupposti indicati nel comma 1 e sussistono particolari motivi di urgenza che non consentono la emissione di un tempestivo decreto di perquisizione.
3. La perquisizione domiciliare può essere eseguita anche fuori dei limiti temporali dell'art. 251 quando il ritardo potrebbe pregiudicarne l'esito.
4. La polizia giudiziaria trasmette senza ritardo, e comunque non oltre le quarantotto ore, al pubblico ministero del luogo dove la perquisizione è stata eseguita il verbale delle operazioni compiute (2572, lett. d). Il pubblico ministero, se ne ricorrono i presupposti, nelle quarantotto ore successive, convalida la perquisizione.

(1) Articolo così modificato dall'art. 9 della L. 48/2008, recante Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno

Le modifiche al C.P.P. a seguito della L. 48/2008

PERQUISIZIONI

247. (Casi e forme delle perquisizioni). 1. Quando vi è fondato motivo di ritenere che taluno occulti sulla persona il corpo del reato (2532) o cose pertinenti al reato, è disposta perquisizione personale. Quando vi è fondato motivo di ritenere che tali cose si trovino in un determinato luogo ovvero che in esso possa eseguirsi l'arresto dell'imputato (60, 61) o dell'evaso, è disposta perquisizione locale (352).

1-bis. Quando vi è fondato motivo di ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino in un sistema informatico o telematico, ancorchè protetto da misure di sicurezza, ne è disposta la perquisizione, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione. (1)

2. La perquisizione è disposta con decreto motivato (1253).

3. L'autorità giudiziaria può procedere personalmente ovvero disporre che l'atto sia compiuto da ufficiali di polizia giudiziaria (57) delegati con lo stesso decreto (370) (2).

(1) Articolo così modificato dall'art. 8, c.2, della L. 48/2008, recante Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno

(2) Cfr. l'art. 68 comma 2 Cost. nonché, per i reati di cui all'art. 90 Cost., l'art. 7, L. 5 giugno 1989, n. 219

L'attività della polizia giudiziaria

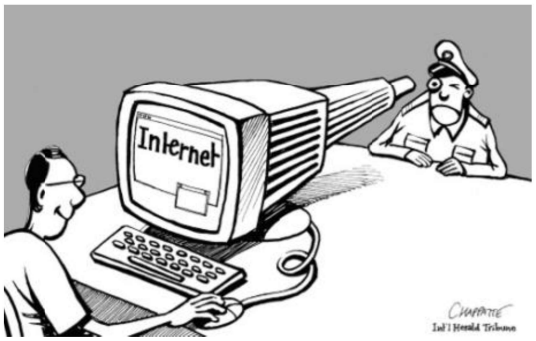
**PERQUISIZIONI DI SISTEMI INFORMATICI,
ON LINE, DA REMOTO A DISTANZA ?**

NO per Corte costituzionale tedesca 370/07 del 27 febbraio 2008

- Diritto all'inviolabilità del domicilio
- Diritto alla segretezza delle comunicazioni
- Diritto alla personalità
- Diritto all'autodeterminazione informativa

- Diritti comprimibili solo a certe condizioni:
  - Rischio per un bene giuridico di rango primario
  - Autorizzazione del giudice
  - Misure idonee a
    - Filtrare
    - Selezionare
    - Cancellare

Intercettazioni di comunicazioni informatiche o telematiche



Le modifiche al C.P.P. a seguito della L. 48/2008

SEQUESTRO DI CORRISPONDENZA TELEMATICA

254. (Sequestro di corrispondenza). [SOSTITUIRE: *1. Negli uffici postali o telegrafici è consentito procedere al sequestro di lettere, pieghi, pacchi, valori, telegrammi e altri oggetti di corrispondenza che l'autorità giudiziaria abbia fondato motivo di ritenere spediti dall'imputato o a lui diretti, anche sotto nome diverso o per mezzo di persona diversa o che comunque possono avere relazione con il reato.* CON]

1. Presso coloro che forniscono servizi postali, telegrafici, telematici o di telecomunicazioni è consentito procedere al sequestro di lettere, pieghi, pacchi, valori, telegrammi e altri oggetti di corrispondenza, anche se inoltrati per via telematica, che l'autorità giudiziaria abbia fondato motivo di ritenere spediti dall'imputato o a lui diretti, anche sotto nome diverso o per mezzo di persona diversa, o che comunque possono avere relazione con il reato.

2. Quando al sequestro procede un ufficiale di polizia giudiziaria (57), questi deve consegnare all'autorità giudiziaria gli oggetti di corrispondenza sequestrati, senza aprirli **o alterarli** e senza prendere altrimenti conoscenza del loro contenuto (353).

3. Le carte e gli altri documenti sequestrati che non rientrano fra la corrispondenza sequestrabile sono immediatamente restituiti all'avente diritto e non possono comunque essere utilizzati (1036) (1).

(1) Articolo così modificato dall'art. 8, c. 4, della L. 48/2008, recante Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno

La registrazione dei dati personali per l'accesso alla Rete

La registrazione dei dati personali per l'accesso alla Rete

Riferimenti normativi:

- D.L. 27 luglio 2005 (c.d. Decreto Pisanu)
- Legge 31 luglio 2005, n. 155 (c.d. Legge Pisanu)
- Decreto Ministero Interno 16 Agosto 2005 (in G.U. n. 190 del 17 agosto 2005)
  Misure di preventiva acquisizione di dati anagrafici dei soggetti che utilizzano postazioni pubbliche non vigilate per comunicazioni telematiche ovvero punti di accesso ad Internet utilizzando tecnologia senza fili, ai sensi dell'art. 7, comma 4, del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155

ABROGATA

La Direttiva (UE) 2016/681 sull'uso dei dati del codice di prenotazione (PNR)

La Direttiva sull'uso dei dati del PNR

Riferimenti normativi:

- **DIRETTIVA (UE) 2016/681 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016 sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confront dei reati di terrorismo e dei reati gravi**

- **Legge 25 ottobre 2017, n. 163, recante delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea - Legge di delegazione europea 2016-2017**

- **DECRETO LEGISLATIVO 21 maggio 2018, n. 53 – Attuazione della direttiva (UE) 2016/681 del Parlamento europeo e del Consiglio, del 27 aprile 2016, sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi e disciplina dell'obbligo per i vettori di comunicare i dati relativi alle persone trasportate in attuazione della direttiva 2004/82/CE del Consiglio del 29 aprile 2004 (GU n.120 del 25-5-2018)**

La Direttiva sull'uso dei dati del PNR

Dati che possono essere presenti in un PNR (https://protezionedatipersonali.it/)

- **numero del passaporto**
- **paese di rilascio del passaporto;**
- **data di scadenza del passaporto;**
- **nome e cognome;**
- **genere;**
- **data e luogo di nascita;**
- **nazionalità;**
- **Passenger Name Record code locator;**
- **data di prenotazione del volo;**
- **altri nomi sul Passenger Name Record (PNR);**
- **indirizzo;**
- **modalità di pagamento;**
- **indirizzo di fatturazione;**
- **numero di telefono;**
- **itinerario completo;**
- **informazioni frequent flyer;**

La Direttiva sull'uso dei dati del PNR

Dati che possono essere presenti in un PNR (https://protezionedatipersonali.it/)

- **agenzia di viaggi;**
- **agente di viaggio;**
- **condivisione codice PNR;**
- **status di viaggio del passeggero;**
- **indirizzo email;**
- **numero del biglietto;**
- **numero di posto;**
- **data di emissione del biglietto;**
- **bagaglio;**
- **richieste di servizio particolari, quali le preferenze dei pasti;**
- **cronistoria delle modifiche del PNR;**
- **numero di viaggiatori nel PNR;**
- **biglietti di sola andata.**

La Direttiva