Diritto all'integrità ed alla confidenzialità del proprio sistema informatico: mito o realtà?

Avv. Giovanni Battista Gallus – Avv. Francesco Paolo Micozzi

E-Privacy - Firenze, 9 e 10 maggio 2008

il Circolo dei Giuristi Telematici

- L'associazione "Circolo dei Giuristi Telematici" è la più "antica" del web giuridico. La storica mailing list conta oggi oltre 200 iscritti tra avvocati, magistrati, giuristi d'impresa, universitari e tecnici specializzati.
- Il sito www.giuristitelematici.it è aggiornato costantemente dai webmaster, anche con la collaborazione di responsabili territoriali, con le principali novità in tema di diritto dell'informatica (e non solo).
- Il Circolo si è fatto promotore di svariati convegni e seminari giuridici, oltre che di alcune pubblicazioni cartacee.
- Le modalità di iscrizione alla mailing list ed all'associazione, lo statuto sociale e il regolamento della mailing list sono consultabili liberamente sul sito. Per ulteriori informazioni: info@giuristitelematici.it. http://www.giuristitelematici.it

Per un diritto costituzionale all'integrità del sistema informatico

Riflessioni sulla sentenza della Corte costituzionale tedesca

Corte Costituzionale Tedesca, sentenza 27/2/2008

Sentenza resa nel procedimento BvR 370/07 - BvR 595/07

Pronunciata dalla Corte Costituzionale Tedesca in data 27/2/2008

Norma soggetta a scrutinio: Legge del Land Nordrhein-Westfalen del 20 dicembre 2006

(I blitz legislativi di fine anno non sono, evidentemente, un'esclusiva italiana)

Legge 20/12/2006

Introduzione di emendamenti ai servizi di intelligence:

- Possibilità di utilizzo di trojan e keyloggers a fini investigativi
- Estese possibilità di investigazione delle comunicazioni via rete
- Internet monitoring
- Richiesta di informazioni su transazioni finanziarie

Legge 20/12/2006

Attività sotto copertura (e non solo)

covertly observe [...] the Internet, especially the covert participation in its communication devices and the search for these, as well as the clandestine access to information-technological systems among others by technical means

Paragrafo 5, n. 11

Bundestrojaner!!

UN TROJAN DI STATO (www.ccc.de)

Corte Costituzionale Tedesca, sentenza 27/2/2008

Ricorrenti:

Bettina Winsemann (giornalista e attivista - www.stop1984.com)

Fabian Brettel (politico - Left Party)

Gerhart Baum (politico - Liberal Party, avvocato, già ministro degli interni)

Julius Reiter e Peter Schantz (avvocati)

Corte Costituzionale Tedesca, sentenza 27/2/2008

I punti critici evidenziati dalla Corte

- Controllo pervasivo dei sistemi
- Superamento dei sistemi di cifratura
- Profilazione dei comportamenti individuali
- Invasione della sfera privata
- Rischio di danni al sistema informatico
- Rischi per i terzi estranei
- Violazione del principio di proporzionalità

Corte Costituzionale Tedesca, sentenza 27/2/2008

“L'uso delle tecnologie dell'informazione ha assunto un significato in precedenza imprevedibile per lo sviluppo della personalità individuale.

Le moderne tecnologie aprono nuove opportunità per gli individui, ma creano nuovi pericoli”

(paragrafo 170)

La risposta della Corte: un nuovo diritto della personalità

La Corte Costituzionale crea un “nuovo” diritto della personalità: il diritto alla integrità e confidenzialità del sistema informatico e telematico

A new "basic right to the confidentiality and integrity of information-technological systems" as part of the general personality rights in the German constitution

http://bendrath.blogspot.com

Aldilà della segretezza delle comunicazioni e dell'inviolabilità del domicilio

La tutela del segreto delle telecomunicazioni (art. 10 della Costituzione tedesca, art. 15 di quella italiana) non può applicarsi ai dati memorizzati sul sistema informatico dell'utente una volta terminata la comunicazione.

“I rischi associati all'infiltrazione nel sistema informatico sono molto maggiori di quelli legati all'intercettazione di comunicazioni e investono anche dati ed informazioni che possono non avere alcun rapporto con attività di natura comunicativa (ossia, possono riguardare anche file o altri elementi che l'utente non ha derivato o utilizzato nel corso delle proprie comunicazioni)”

Giuseppe Briganti, http://iusreporter.blogspot.com

Aldilà della segretezza delle comunicazioni e dell'inviolabilità del domicilio

Non basta neanche il diritto all'inviolabilità del domicilio (art. 13 della Cost. Tedesca, art. 14 di quella italiana), poiché si prescinde del tutto dalla localizzazione fisica del sistema informatico o telematico

“Si tratta, dunque, di ripensare ai diritti della personalità, includendovi il nuovo diritto all'integrità e riservatezza dei sistemi telematici qualora i rischi connessi ad un accesso da parte di terzi - come nel caso in oggetto - siano tali da permettere una profilazione "spinta" dell'individuo o l'acquisizione di informazioni a tutto campo che incidono sul libero sviluppo della sua personalità”

Giuseppe Briganti, http://iusreporter.blogspot.com

Sistemi informatici come espressione della personalità

"From the relevance of the use of information-technological systems for the expression of personality (Persönlichkeitsentfaltung) and from the dangers for personality that are connected to this use **follows a need for protection that is significant for basic rights**.

The individual is depending upon the State respecting the justifiable expectations for the integrity and confidentiality of such systems with **a view to the unrestricted expression of personality**." (margin number 181)

Trad. Ralf Bendrath

Sistemi informatici come espressione della personalità

Viene completato il quadro dei diritti fondamentali già enucleati dalla Corte:

Il Diritto all'autodeterminazione informativa (1983)

Il Diritto alla protezione assoluta del nucleo inviolabile della propria vita privata (2004).

A new right is born

An existing right to freedom in telecommunications was too narrow; legal protections surrounding a private home included home computers but not laptops carried in public, electronic organizers or mobile phones. The right to 'protection of the private sphere' and 'informational self-determination' have protected computer users so far, but insufficiently.

So the verdict in the online-surveillance case has created a whole new basic right ... **In shorthand (it might be called) the 'IT right'**

Dietmar Hipp, Spiegel online

A new right is born

“Il certificato di nascita di questo nuovo diritto è lungo 106 pagine, e i giudicanti continuano a ripeterne il suo nome, come se volessero instillarlo nella coscienza politica della Germania”

Süddeutsche Zeitung

Dobbiamo fidarci dei nostri sistemi informatici!

- L'indiscriminata raccolta di informazioni colpisce indirettamente la libertà dei cittadini per il timore di essere sorvegliati (paragrafo 233)
- Computer users have the right to trust their IT equipment
  - **http://www.spiegel.de/international/germany/0,1518,538378,00.html**
- Germany puts legal firewall around computers
  - http://www.monstersandcritics.com/tech/news/article_1393159.php

Dobbiamo fidarci dei nostri sistemi informatici!

Dichiarazione del Ministro della Giustizia Brigitte Zypries:

“The ruling will foster trust in the integrity of information technology systems”

Fonte: Bloomberg

Quali sistemi godono della protezione?

Godono di protezione i sistemi che "alone or in their technical interconnectedness can contain personal data of the affected person in a scope and multiplicity such that **access to the system makes it possible to get insight into relevant parts of the conduct of life of a person or even gather a meaningful picture of the personality.**" (margin number 203)

Quindi non solo i pc, ma anche PDA e smartphone

Un diritto assoluto?

Questo diritto può essere violato solo se vi è il concreto pericolo della commissione di gravi reati, con l'intervento dell'Autorità Giudiziaria, e solo laddove le altre risorse investigative si dimostrino insufficienti

Ma anche in questo caso, **occorre proteggere l'area della vita privata**

"If there are concrete indications in the specific case that a certain measure for gathering data will touch the core area of the conduct of private life, it has to remain principally undone." (margin number 281)

Se comunque venissero accidentalmente acquisiti dati afferenti tale “core area”, essi devono essere immediatamente cancellati, e non possono essere utilizzati in nessun modo

L'età dell'informazione

“The constitutional court has arrived in the information age"

Gerhart Baum, dichiarazione a Der Spiegel

“La Corte Costituzionale Federale ha dotato l'ego virtuale di uno scudo protettivo digitale”

Dirk Engling, ccc.de

E la in Italia? Siamo ancora distanti, anche se Vittorio Frosini, sin dal 1981, aveva sviluppato la “dottrina della libertà informatica”.

Il cyberego

“Il corpo di ciascuno di noi si allarga fino a comprendere gli strumenti tecnologici di cui ci serviamo nella vita quotidiana

La Corte Costituzionale tedesca non rafforza solo la garanzia giuridica. **Crea una nuova antropologia**.

Su questo nuovo corpo, insieme fisico e tecnologico, non si possono mettere le mani.

Nasce un nuovo *habeas corpus*”

Stefano Rodotà, La Repubblica, 22/3/2008

In conclusione...

Philip K. Dick si chiedeva

Do androids dream of electric sheep?

Ora ci si potrebbe chiedere

Will netizens dream of digital shields?

Sitografia minima

http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html

(Testo integrale della sentenza, in tedesco)

http://bendrath.blogspot.com/2008/02/germany-new-basic-right-to-privacy-of.html

http://www.spiegel.de/international/germany/0,1518,538378,00.html

http://www.ccc.de/updates/2008/trojaner-notschlachten?language=en

http://www.deutsche-welle.de/dw/article/0,2144,3152627,00.html

http://www.edri.org/edrigram/number6.4/germany-constitutional-searches

http://www.heise-online.co.uk/news/German-Constitutional-Court-rejects-government-snooping-of-PC

http://www.nytimes.com/2008/02/28/world/europe/28germany.html?ref=world

http://www.lg2g.info/modules/news/article.php?storyid=357&location_id=5

http://www.monstersandcritics.com/tech/news/article_1393159.php

http://iusreporter.blogspot.com/2008/03/per-la-corte-costituzionale-tedesca-on.html

Cripto ergo sum!

nemo tenetur se detegere... ed altre amenità

I file cifrati del signor Boucher

La disavventura di *Sebastien Boucher* ha inizio alla frontiera del Canada, quando gli agenti doganali decidono di controllare il suo laptop. Gli agenti doganali venivano insospettiti dalla presenza di alcuni file il cui nome induceva a ritenere che si trattasse di materiale di tipo pedopornografico.

I file, però, erano protetti da un sistema di cifratura (PGP) e gli agenti non avrebbero potuto prendere visione dei contenuti digitali senza la “collaborazione” del signor Boucher, che avrebbe, in sostanza, dovuto rivelare la chiave d'accesso ai file cifrati.

I file cifrati del signor Boucher

Occorre, preliminarmente, premettere che di recente il controllo sui file contenuti in un computer è stato ritenuto perfettamente lecito anche nell'ipotesi in cui il soggetto sul quale i controlli siano eseguiti non desti alcun particolare motivo di sospetto.

Al riguardo, infatti, è intervenuta recentemente (21 aprile 2008) la sentenza della Corte d'Appello degli Stati Uniti, nel processo contro Michael Timothy Arnold, secondo la quale quando si tratti di controlli alla frontiera non è necessario che ci si trovi di fronte ad un “legittimo sospetto”.

I file cifrati del signor Boucher

Cosa avrebbe dovuto fare il signor Boucher?

- Rivelare la chiave e dare, di conseguenza, la certezza della detenzione di materiale illecito?

Oppure

- tacere, evitando, così, di autoaccusarsi?

Il signor Boucher optò per la seconda soluzione. Oltretutto tale scelta era – secondo Boucher – un'estrinsecazione del diritto derivante dal quinto emendamento della Costituzione degli Stati Uniti d'America.

Il quinto emendamento

No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offense to be twice put in jeopardy of life or limb; ***nor shall be compelled in any criminal case to be a witness against himself****, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation.*

TRAD. "nè essere obbligato a deporre, in un procedimento penale, contro di sé"

Il quinto emendamento... italiano

- No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger;
- nor shall any person be subject for the same offense to be twice put in jeopardy of life or limb;
- **nor shall be compelled in any criminal case to be a witness against himself**,
- nor be deprived of life, liberty, or property, without due process of law;

- L'imputato non è considerato colpevole sino alla condanna definitiva (art. 27 co II Cost.)
- Principio del *ne bis in idem*
- ***La Repubblica riconosce e garantisce i diritti inviolabili dell'uomo, sia come singolo sia nelle formazioni sociali ove si svolge la sua personalità [...]*** *(art. 2 Cost.), ed anche* ***La difesa è diritto inviolabile in ogni stato e grado del procedimento*** *(art. 24 co II Cost.)*
- [...] Nessuno può essere punito se non in forza di una legge che sia entrata in vigore prima del fatto commesso [...] (art. 25 Cost)

Il nostro codice di proc. penale

Art. 198, comma II c.p.p.

Il testimone non può essere obbligato a deporre su fatti dai quali potrebbe emergere una sua responsabilità penale.

Anche questa norma è espressione del principio costituzionale di cui al combinato disposto degli artt. 24, II co. e 2 Cost.. In sostanza se la norma di cui al 198 c.p.p. non fosse esistita sarebbe, comunque, incostituzionale ogni altra norma che prevedesse il contrario.

L'art. 199 cpp prevede, invece, la facoltà di astensione per I prossimi congiunti (con alcune eccezioni)

Giudice, PM e PG...

Sebbene la previsione di cui all'art. 198, II co., cpp ha come destinatario il giudice (nel senso che la norma vieta al giudice di costringere il soggetto a parlare > inutilizzabilità), essa opera anche con riferimento al pubblico ministero (362 cpp mediante il richiamo all'art. 198 cpp) ed alla polizia giudiziaria (351 cpp mediante il richiamo all'art. 362 cpp)

Dal sospetto al processo

- La difesa è un diritto inviolabile in ogni stato e grado del procedimento.
- Il signor Boucher, in Italia, si sarebbe visto sequestrare il portatile; sarebbero state svolte indagini sul computer (art. 360 c.p.p.); il pubblico ministero, all'esito delle indagini preliminari, avrebbe potuto chiedere – eventualmente – il rinvio a giudizio. Tutto secondo le ordinarie regole del processo penale.

Art. 63 cpp

Dichiarazioni indizianti.

1. Se davanti all'autorità giudiziaria o alla polizia giudiziaria una persona non imputata ovvero una persona non sottoposta alle indagini rende dichiarazioni dalle quali emergono indizi di reità a suo carico, l'autorità procedente ne interrompe l'esame, avvertendola che a seguito di tali dichiarazioni potranno essere svolte indagini nei suoi confronti e la invita a nominare un difensore. Le precedenti dichiarazioni non possono essere utilizzate contro la persona che le ha rese.
2. Se la persona doveva essere sentita sin dall'inizio in qualità di imputato o di persona sottoposta alle indagini, le sue dichiarazioni non possono essere utilizzate.

False informazioni...

- Non è previsto, nel nostro Ordinamento, il reato di false informazioni alla Polizia Giudiziaria*;
- E' previsto unicamente il reato di false informazioni al pubblico ministero ed al difensore.
  - Problema: la richiesta del PM non ottemperata di rivelare una password è astrattamente inquadrabile nel reato di cui all'art. 371 *bis* c.p.?

[I]. Chiunque, nel corso di unproce

Art. 371 bis c.p. False informazioni al pubblico ministero

- *Chiunque, nel corso di un procedimento penale, richiesto dal pubblico ministero di fornire informazioni ai fini delle indagini, rende dichiarazioni false ovvero tace, in tutto o in parte, ciò che sa intorno ai fatti sui quali viene sentito, è punito con la reclusione fino a quattro anni.*
- *Ferma l'immediata procedibilità nel caso di rifiuto di informazioni, il procedimento penale, negli altri casi, resta sospeso fino a quando nel procedimento nel corso del quale sono state assunte le informazioni sia stata pronunciata sentenza di primo grado ovvero il procedimento sia stato anteriormente definito con archiviazione o con sentenza di non luogo a procedere.*
- *Le disposizioni di cui ai commi primo e secondo si applicano, nell'ipotesi prevista dall'art. 391-bis, comma 10, del codice di procedura penale, anche quando le informazioni ai fini delle indagini sono richieste dal difensore.*

Art. 384 c.p. - Casi di non punibilità

- *Nei casi previsti dagli articoli 361, 362, 363, 364, 365, 366, 369, 371-bis, 371-ter, 372, 373, 374 e 378, non è punibile chi ha commesso il fatto per esservi stato costretto dalla* ***necessità di salvare se medesimo o un prossimo congiunto da un grave e inevitabile nocumento nella libertà*** *o nell'onore.*
- *Nei casi previsti dagli articoli 371-bis, 371-ter, 372 e 373, la* ***punibilità è esclusa se il fatto è commesso da chi per legge non avrebbe dovuto essere richiesto di fornire informazioni ai fini delle indagini o assunto come testimonio****, perito, consulente tecnico o interprete* ***ovvero non avrebbe potuto essere obbligato a deporre o comunque a rispondere o avrebbe dovuto essere avvertito della facoltà di astenersi dal rendere informazioni, testimonianza****, perizia, consulenza o interpretazione.*

Riepiloghiamo il problema:

La richiesta del PM non ottemperata di rivelare una password è astrattamente inquadrabile nel reato di cui all'art. 371 bis c.p.?

- Quando potrà dirsi che il soggetto che si è rifiutato di comunicare la password (o che ne ha comunicato una sbagliata) non sarà punibile ex art. 384 c.p.?
  - In modo assoluto nel momento in cui si scoprirà effettivamente il contenuto del file cifrato.
  - Ricordiamo, inoltre, che nel processo penale non esistono prove

Il limite del *nemo tenetur*...

Tornando all'art. 198, secondo comma, c.p.p. è necessario però ricordare che, per opporre il privilegio contro l'autoincriminazione, bisogna **dare una giustificazione allo stesso**.

Ciò significa che non si può tacere ed opporre *sic et simpliciter* il privilegio. Bisogna, invero, **dimostrare di trovarsi in una situazione legittimante... senza dimostrare troppo!**

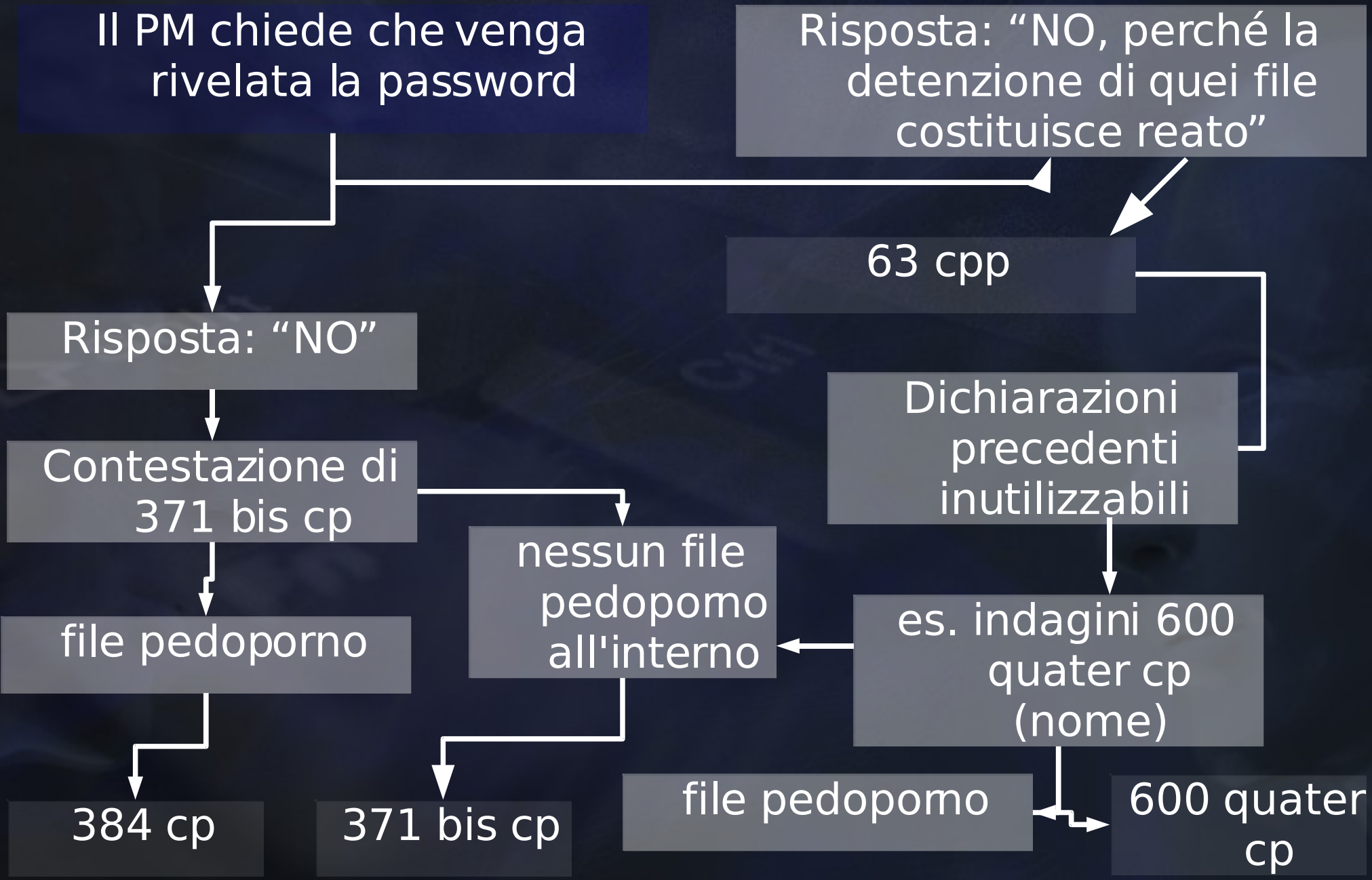
La non punibilità del 384 cp

- Ipotizziamo che il nostro Boucher dica: “Non vi svelo la password perché la detenzione dei file cifrati costituisce reato (o perché subirei un nocumento nell'onore” (anche se il “nocumento” può derivare – per giurisprudenza pacifica – anche dall'applicazione di sanzioni amm.ve*).
  - Se Boucher non dimostra quali file vi siano celati all'interno del file cifrato il PM non potrà qualificare giuridicamente la fattispecie concreta: potrebbe infatti trattarsi di file pedopornografici, di file protetti dalle norme sul diritto d'autore, etc.

E se non ricorda la password?

- Anche a voler ritenere integrato il reato di false informazioni al PM nel caso in cui taluno non voglia rivelare la password di accesso ad un file cifrato (potendo, astrattamente, ritenersi questa informazione rientrante nel disposto di cui all'art. 371 bis cp) cosa succederebbe nel caso in cui, invece, il soggetto non possa (perché non la ricorda) rivelare la password?

Un esempio...


Il PM chiede che venga rivelata la password
Risposta: “NO, perché la detenzione di quei file costituisce reato”
63 cpp
Risposta: “NO”
Contestazione di 371 bis cp
Dichiarazioni precedenti inutilizzabili
nessun file pedopomo all'interno
file pedoporno
es. indagini 600 quater cp (nome)
384 cp
371 bis cp
file pedopomo
600 quater cp

Una precisazione doverosa...

- Nello schema appena visto, la configurabilità del reato previsto dall'art. 371 bis cp rappresenta la “peggiore” delle ipotesi prospettabili.
- In effetti oggetto della richiesta del PM non sarebbe “ciò che sa intorno ai fatti” (oggetto dell'indagine), ma ciò che non deriva dalla percezione della realtà fenomenica.

Quando criptare è reato...

- In alcuni casi non è necessario che sia richiesta una password per dimostrare un reato. E' sufficiente detenere software per la cifratura dei dati!
- E' una situazione differente da quella prospettata dalla RIPA inglese, però si crea un reato di sospetto.

Avviso orale e sistemi di cifratura

- Legge n. 1423 del 27 dicembre 1956
- Articolo 4

  *** COMMA IV - Con l'avviso orale il questore, quando ricorrono le condizioni di cui all'articolo 1, può imporre alle persone che risultino definitivamente condannate per delitti non colposi il divieto di possedere o utilizzare, in tutto o in parte, qualsiasi apparato di comunicazione radiotrasmittente, radar e visori notturni, indumenti e accessori per la protezione balistica individuale, mezzi di trasporto blindati o modificati al fine di aumentarne la potenza o la capacità offensiva, ovvero comunque predisposti al fine di sottrarsi ai controlli di polizia, nonché **programmi informatici ed altri strumenti di cifratura o crittazione di conversazioni e messaggi**. Il divieto del questore è opponibile davanti al giudice monocratico.

  COMMA V - Chiunque violi il divieto di cui al quarto comma è punito con la reclusione da uno a tre anni e con la multa da lire tre milioni a lire dieci milioni. Gli strumenti, gli apparati, i mezzi e i programmi posseduti o utilizzati sono confiscati ed assegnati alle Forze di polizia, se ne fanno richiesta, per essere impiegati nei compiti di istituto.

  *** Il quarto comma è stato introdotto dalla L. 327/1988 e successivamente

L'avviso orale

- E' una misura di prevenzione disposta con un atto amministrativo discrezionale del Questore.
- E' emanato sulla base di una prognosi di pericolosità sociale di determinate persone.
- Ha una “durata” limitata a tre anni.
- Non è direttamente impugnabile in sede giurisdizionale.

Il reato di sospetto

- il reato di cui al comma quinto dell'art. 4 L 1423/56 rappresenta un reato c.d. “di sospetto”, che fornisce di una forma di estrema anticipazione della tutela penale per taluni beni giuridici .
- E' possibile fare un parallelismo con l'art. 707 cp, e ritenere che anche quello in oggetto rientri nell'ambito dei “reati ostativi', «cioè di quelle incriminazioni, lontanamente arretrate, che non colpiscono comportamenti offensivi di un bene, ma tendono a prevenire il realizzarsi di azioni effettivamente lesive o pericolose, mediante la punizione di atti che sono la premessa idonea per la commissione di altri reati».

Altri strumenti di cifratura

Enigma!

Altri strumenti di cifratura

GPG? Chevvordì?

Paralleli

- Il reato in questione, in sostanza, è in parte identico alla contravvenzione stabilita dall'art. 707 cp.
- Ma il 707 richiede che il porto debba essere “non giustificato”, la norma di cui all'art. 4, quinto comma, L. 1423/56 no.
- il pericolo è inteso in modo assoluto.

Non ho nulla da nascondere...

«Bisogna diffidare dell'argomento di chi sottolinea come il cittadino probo non abbia nulla da temere dalla conoscenza delle informazioni che lo riguardano.

«“*L'uomo di vetro*” è una metafora totalitaria, perché su di essa si basa poi la pretesa dello Stato di conoscere tutto, anche gli aspetti più intimi della vita dei cittadini, trasformando automaticamente in “sospetto” chi chieda salvaguardia della vita privata.»

Grazie per l'attenzione

g.gallus@studiogallus.it - f.micozzi@studionati.it