# Internet e censura nella Pubblica Amministrazione

*Ricerca sulla inibizione della navigazione dei dipendenti pubblici sul posto di lavoro*

di Antonio Prado
https://www.prado.it
10 gennaio 2016

## Sommario

*Nell'ordinamento italiano è stabilito che gli operatori di rete debbano inibire l'accesso di tutti gli utenti a numerose risorse Internet. Ho voluto indagare se e quanto queste misure siano applicate all'interno degli uffici pubblici. A questo scopo è stato predisposto un breve questionario sottoposto, nel mese di dicembre 2015, agli operatori ICT degli enti pubblici italiani. Nel presente documento vengono presentati, spiegati e commentati i risultati dell'indagine.*

# Indice

# Licenza

# Cos'è la censura su Internet (in Italia)

Il concetto di censura non va di certo spiegato, ne riporto però la definizione pubblicata on-line dall'enciclopedia Treccani[1] come punto di partenza per una riflessione:

> *"Limitazione della libertà civile di espressione del pensiero, disposta per la tutela di un interesse pubblico e attuata mediante l'esame, da parte di un'autorità, di scritti o giornali da stamparsi, di manifesti o avvisi da affiggere in pubblico, di opere teatrali o pellicole da rappresentare, di siti Internet, con lo scopo di permetterne o vietarne la pubblicazione, l'affissione, la rappresentazione ecc."*

Restringiamo l'ambito alle risorse di Internet e riconosciamo due momenti distinti nell'applicazione della censura:

- la **pubblicazione** dei contenuti;
- la **fruizione** dei contenuti.

Cioè è possibile nel primo caso censurare evitando che il contenuto sia diffuso on-line (o oscurandolo nel caso in cui sia già stato pubblicato), nel secondo caso applicando una inibizione agli utenti di Internet che impedisca loro l'accesso al contenuto censurato.

Da una parte l'autorità agisce sui server di *hosting*, quelli che ospitano cioè i contenuti oggetto della censura, ordinando un sequestro; dall'altra l'autorità comanda ai fornitori di accesso a Internet di dirottare le richieste degli utenti verso pagine esplicative del provvedimento di censura, di fatto impedendone la fruizione.

## Perché la censura

Alla base della censura su Internet, in Italia (così come in altri Paesi europei[2]), ci sono delle norme che hanno l'obiettivo di difendere **interessi della collettività** (a esempio il contrasto della pornografia infantile) o **interessi di singoli** (come la difesa del diritto d'autore).

Norme che mirano a perseguire l'obiettivo di inibire l'accesso a determinate risorse di Internet indistintamente per chiunque sia soggetto all'ordinamento italiano: privati cittadini, aziende, pubbliche amministrazioni.

[1] Enciclopedia Treccani, *Definizione di censura*: http://www.treccani.it/enciclopedia/censura/

[2] S. Bortzmeyer, *DNS Censorship (DNS Lies) As Seen By RIPE Atlas*: https://labs.ripe.net/Members/stephane_bortzmeyer/dns-censorship-dns-lies-seen-by-atlas-probes

# Fonti normative


## Centro nazionale per il contrasto alla pedo-pornografia on-line[3] (CNCPO): Legge 38 del 6 febbraio 2006[4]

Questa legge istituisce il Centro nazionale per il contrasto alla pedo-pornografia su Internet (CNCPO) presso il Servizio Polizia postale e delle comunicazioni del Dipartimento della Pubblica Sicurezza.

La struttura ha il compito di condurre una continua sorveglianza alla ricerca di siti web e frangenti che possano costituire un pericolo per i ragazzi, come commercio on-line di immagini o filmati di **minori abusati sessualmente**. Per questo ultimo aspetto in particolare, il CNCPO agisce da raccordo per le segnalazioni che possono provenire da altre forze di polizia (anche straniere), da semplici cittadini o da fornitori di servizi Internet.

Tale attività è in grado di produrre un elenco dei siti web in qualche modo correlati alla pedo-pornografia, una vera e propria *black list*, per comprensibili motivi non pubblicamente disponibile, che gli operatori di rete devono richiedere per poter inibire la navigazione dei loro utenti. La violazione di questo obbligo comporta una sanzione amministrativa che va da 50mila a 250mila euro.


## Agenzia delle dogane e dei monopòli[5] (ADM): Decreto direttoriale 2 gennaio 2007[6]

La norma è pensata per tutti quei siti web che, **senza autorizzazione**, offrono la possibilità di effettuare giochi, scommesse o concorsi pronostici on-line con vincite in denaro.

Ne risulta, a carico dei fornitori di accesso a Internet, una attività obbligatoria di inibizione di una lista di siti Internet redatta dall'agenzia stessa e messa a disposizione pubblicamente[7].

Ferma restando l'eventuale responsabilità penale dei fornitori di servizi di rete, le violazioni dell'obbligo di inibizione sono punite con una sanzione amministrativa da 30mila a 180mila euro.

---

[3] Centro nazionale per il contrasto alla pedo-pornografia on-line: http://www.poliziadistato.it/articolo/23399/

[4] Ordinamento italiano, *Legge 38 del 6 febbraio 2006*: http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2006-02-06;38!vig=

[5] Agenzia delle dogane e dei monopòli: http://www.agenziadoganemonopoli.gov.it/

[6] Agenzia delle dogane e dei monopòli, *Decreto direttoriale 2 gennaio 2007*: http://www1.agenziadoganemonopoli.gov.it/files_monopoli/documenti_old/private/downloads/documentazione/scommesse/Decreti_siti_illegali/Decreto_Direttoriale_2_gennaio_2007.pdf

[7] Agenzia delle dogane e dei monopòli, *black list*: https://www1.agenziadoganemonopoli.gov.it/files_siti_inibiti/elenco_siti_inibiti.txt

## Autorità per le garanzie nelle comunicazioni[8] (AGCOM): Delibera 680/13/CONS del 12 dicembre 2013[9]

Il regolamento, in vigore dal 31 marzo 2014, definisce le modalità di accertamento e di cessazione delle **violazioni del diritto d'autore** e dei diritti connessi.

Qualora il sito web sul quale sono rese disponibili opere digitali in violazione del diritto d'autore o dei diritti connessi sia ospitato su un server ubicato nel territorio italiano, l'autorità ordina al fornitore di *hosting* di rimuoverle. In presenza di violazioni di carattere massivo l'autorità può ordinare la disabilitazione dell'accesso a quelle opere digitali.

Se invece il sito web è ospitato su un server ubicato fuori dal territorio nazionale, l'autorità può ordinare agli operatori di rete di provvedere alla disabilitazione dell'accesso per tutti gli utenti.

A ogni delibera di AGCOM in materia di tutela del diritto d'autore viene allegato un elenco[10] di tutte le URL che gli operatori di rete devono inibire.

## Decreti dell'Autorità giudiziaria

In qualsiasi momento è possibile che una Procura della Repubblica emani un decreto di **sequestro preventivo** di una risorsa Internet non solo nelle modalità già illustrate, cioè sequestrando i server che erogano i contenuti oppure ordinando ai fornitori di accesso a Internet di inibire l'accesso a determinati contenuti per tutti i loro utenti.

Alcuni decreti[11] riportano la dicitura:

> *"sequestro degli Indirizzi IP statici che al momento risultano associati ai predetti domini nonché ad ogni ulteriore indirizzo associato al nome stesso nell'attualità e nel futuro".*

Dunque, non solo l'inibizione dei nomi dei siti web oggetto dell'attenzione degli inquirenti, ma anche gli indirizzi numerici (IP) che in qualsiasi tempo e luogo siano associati a quei nomi (fino ovviamente all'ordine di dissequestro).

[8] Autorità per le garanzie nelle comunicazioni: http://www.agcom.it/

[9] Autorità per le garanzie nelle comunicazioni, *Delibera 680/13/CONS del 12 dicembre 2013*: http://www.agcom.it/documents/10179/540163/Delibera+680-13-CONS/2fb37939-620c-410d-a23f-2150d505b103?version=1.1

[10] Autorità per le garanzie nelle comunicazioni, *black list*: http://www.agcom.it/documents/10179/3329326/Allegato+18-12-2015+1450453953614/716b21b1-d3e4-4af2-a4e3-16872fc22544?version=1.0

[11] GIP Ghinetti Tribunale di Milano, *Decreto di sequestro preventivo*: http://www.penalecontemporaneo.it/upload/1362735944SequestroPreventivoSitiFlor.pdf

### Presidenza del Consiglio dei Ministri, Dipartimento della Funzione Pubblica[12]: Direttiva 2 del 26 maggio 2009[13]

Nella Pubblica Amministrazione questo testo firmato dall'allora ministro Renato Brunetta è molto conosciuto. Si raccomanda alle amministrazioni di dotarsi di software idonei a impedire l'accesso a siti Internet aventi contenuti e/o finalità vietati dalla legge: visione di siti non pertinenti, upload e download di file, uso di servizi di rete con finalità ludiche o comunque estranee all'attività lavorativa.

La direttiva dunque pone in capo al datore di lavoro pubblico il compito di censurare fortemente l'accesso dei dipendenti pubblici a Internet, ma si astiene dal fornire indicazioni operative così che sarà responsabilità di ciascuna Amministrazione tratteggiare il perimetro di applicazione della censura.

In altre parole, ai dipendenti pubblici non solo si deve applicare la specifica inibizione comune a tutti i cittadini italiani (precedentemente enumerata), ma anche una ulteriore e **discrezionale censura** su tutte le risorse Internet eccetto su quelle necessarie per espletare l'attività lavorativa.

## Censura che si basa su DNS

Le cosiddette *black list* formulate da CNCPO, ADM, AGCOM e da alcuni decreti dell'Autorità giudiziaria devono essere utilizzate per reindirizzare la navigazione degli utenti verso apposite pagine contenenti un testo esplicativo del motivo dell'inibizione. In questi casi le norme e i regolamenti prevedono, per la fattiva realizzazione del blocco, l'uso del **server risolutore dei nomi** (DNS).

[12] Dipartimento della Funzione pubblica: http://www.funzionepubblica.gov.it/

[13] Dipartimento della Funzione pubblica, *Direttiva 2 del 26 maggio 2009*: http://www.funzionepubblica.gov.it/media/339454/direttiva_n2_09.pdf


## Cos'è il DNS[14]

Semplificando, il DNS, *domain name system*, è un servizio di traduzione dei nomi a dominio di Internet in indirizzi numerici (IP). Gli indirizzi IP, *internet protocol*[15], sono identificativi univoci dei calcolatori presenti su Internet.

Per questo, ogni qual volta decidiamo di visitare il sito web http://www.example.org, il nostro calcolatore chiede al server DNS (precedentemente e, nella maggior parte dei casi, automaticamente impostato) a quale indirizzo IP corrisponda il nome a dominio www.example.org.

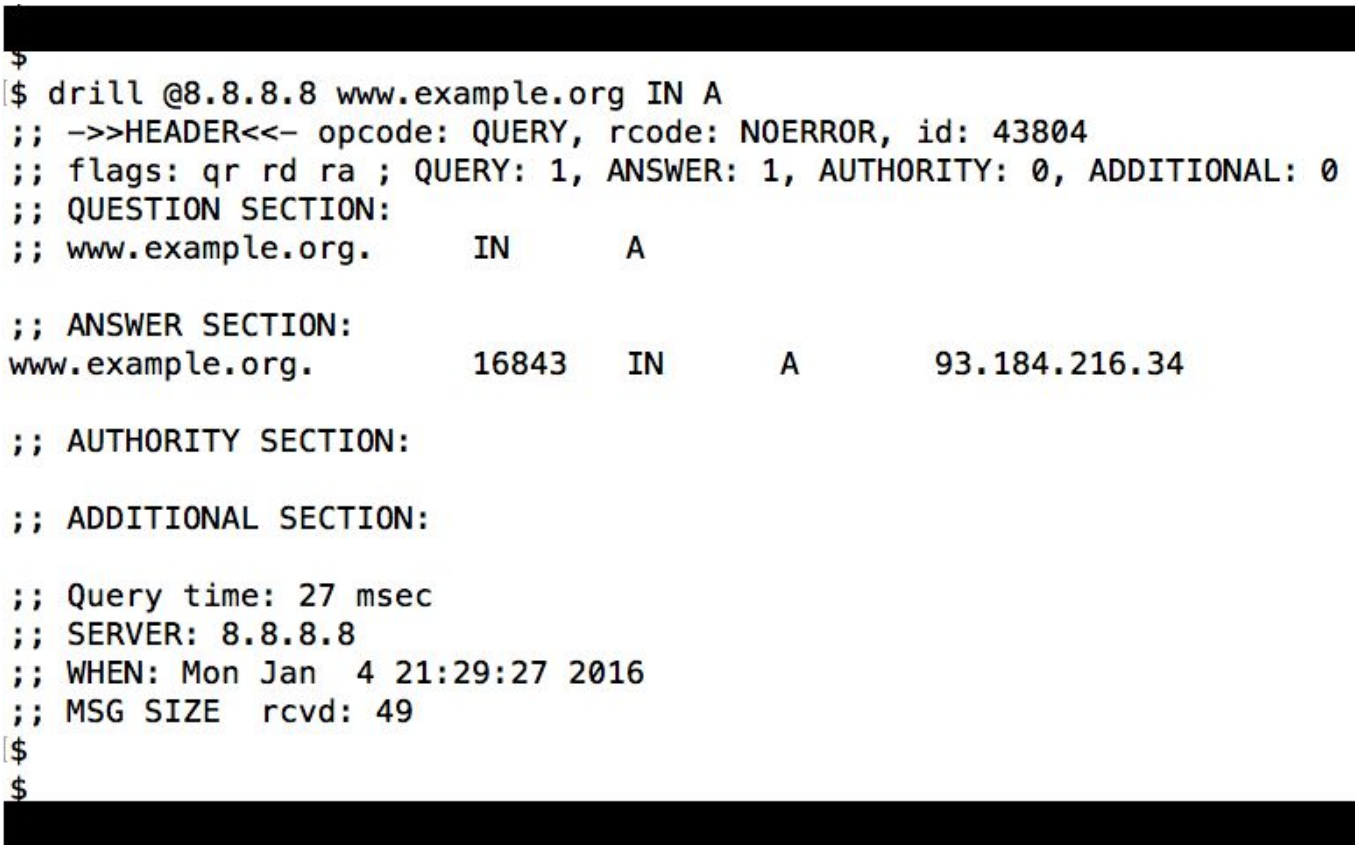
Il server DNS che andiamo a interrogare risponderà, molto probabilmente, con codici numerici (IP) del tipo:

> *203.0.113.1*
>
> *oppure*
>
> *2001:DB8:1234:5678:9ABC:DEF::1*

Solo a quel punto il nostro calcolatore sarà in grado di collegarsi e mostrarci il contenuto di http://www.example.org.

[14] P. Mockapetris, *Domain Names - Implementation and specification*: https://www.rfc-editor.org/rfc/rfc1035.txt

[15] J. Postel, *Internet Protocol*: https://www.rfc-editor.org/rfc/rfc791.txt




Ora, è facilmente comprensibile come controllare i server DNS sia una funzione altamente delicata e di fiducia poiché, manomettendo le risposte che il DNS dà, è possibile indirizzare a piacimento la navigazione altrui.[16]

Ed è proprio in questo meccanismo che il legislatore ha deciso di interferire per l'applicazione della censura. Quindi gli operatori di rete che offrono un servizio di connettività, e forniscono plausibilmente anche dei server DNS ai clienti, hanno l'obbligo di **manipolare le risposte** alle domande di quei calcolatori che richiedono la traduzione dei nomi presenti nelle liste di inibizione così da indirizzarli verso pagine predisposte dalle autorità anziché verso l'originale (e illegale) sito web richiesto.

## Censura che si basa sul dirottare gli instradamenti di Internet

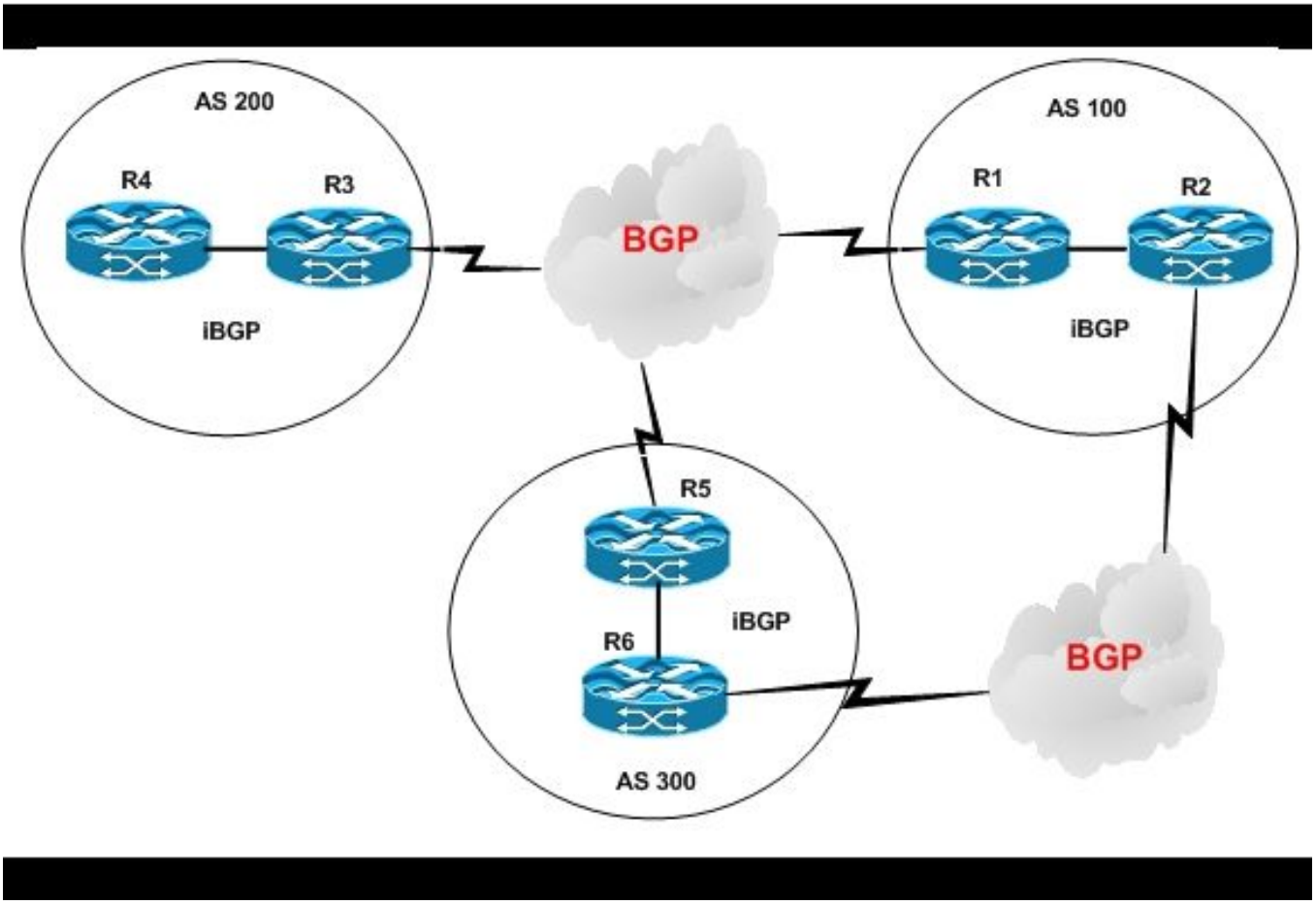
Alcuni decreti dell'Autorità giudiziaria, come già accennato, non si sono limitati a ordinare la censura dei siti web oggetto del sequestro attraverso la tecnica, appena esposta, della manomissione del DNS. Hanno invece ulteriormente esteso l'inibizione agli indirizzi IP ai quali quei siti sono legati sia al momento della redazione del decreto sia agli eventuali indirizzi IP ai quali quei siti web, in futuro, si legassero.

[16] H. Shulman, A. Herzberg, *DNS Cache-Poisoning: New Vulnerabilities*: https://www.ietf.org/proceedings/87/slides/slides-87-saag-3.pdf

La questione, da un punto di vista squisitamente operativo, assume un profilo *sui generis* poiché richiede che gli operatori di rete iniettino, dinamicamente, gli indirizzi IP provenienti dalle *black list* all'interno dei loro dispositivi per l'instradamento (*router*).

## Cos'è l'instradamento di Internet[17]

Tentando di abbreviare una storia lunga, dirò che Internet è costituita di migliaia di **sistemi autonomi**[18] (AS, *autonomous system*), cioè l'insieme delle risorse IP rispondente a un operatore di rete, che interconnettono le proprie infrastrutture gli uni agli altri usando il protocollo BGP[19], *border gateway protocol,* secondo un criterio unico e chiaramente definito.




[17] S. Halabi, *Internet routing architectures 2nd edition*: http://www.ciscopress.com/store/internet-routing-architectures-9781578702336

[18] J. Hawkinson, T. Bates, *Guidelines for creation, selection, and registration of an Autonomous System (AS)*: https://www.rfc-editor.org/rfc/rfc1930.txt

[19] K. Lougheed, Y. Rekhter, *A Border Gateway Protocol (BGP)*: https://www.rfc-editor.org/rfc/rfc1163.txt

Ciascun sistema autonomo ha il compito di rendere raggiungibili le proprie risorse IP a tutti gli altri sistemi autonomi del mondo e, viceversa, di indicare ai propri utenti la strada per raggiungere le risorse IP di tutti gli altri AS.

Le autorità giudiziarie hanno, in diversi casi, ordinato che gli operatori di rete intervenissero proprio su questi criteri di instradamento degli indirizzi IP (gestiti attraverso il protocollo BGP) così da generare un vero e proprio **dirottamento delle richieste** degli utenti. Una modalità utilizzata anche in altri Paesi[20].

In altre parole, riprendendo l'esempio fatto sopra, un calcolatore che volesse connettersi a http://www.example.org, andrebbe a domandare al server DNS la traduzione del nome a dominio in IP ma, una volta ottenuto l'indirizzo numerico non sarebbe in grado di raggiungerlo poiché l'instradamento che normalmente l'operatore di rete garantisce, verrebbe interrotto o addirittura dirottato verso una diversa (e innocua) destinazione.

Un orientamento, questo partorito da alcune autorità giudiziarie, che ha provocato accese critiche da parte dei più attenti osservatori delle *res ætheris*.[21]

In effetti, considerato che a ciascun singolo indirizzo IP possono essere legate enormi quantità di siti web (come consentito dal protocollo standard HTTP 1.1[22]), il rischio di tali decreti sarebbe quello di impedire l'accesso anche a una moltitudine di risorse Internet che nulla ha a che vedere con il sito web oggetto del sequestro, configurando una evidente **sproporzionalità tra l'obiettivo perseguito e il provvedimento adottato**. Tali risorse hanno solo la malasorte di condividere l'indirizzo IP con il nome a dominio nel mirino delle autorità.

Ora, volendo confrontare le due diverse tecniche esposte, si può concludere che la misura della manomissione del DNS è facilmente superabile dall'utente finale (di una P.A. e no) impostando (manualmente) dei valori corrispondenti a server non soggetti alle norme italiane, a esempio i servizi di risoluzione dei nomi pubblici e gratuiti messi a disposizione da Google o da Cisco (almeno finché il loro uso sarà consentito).

D'altronde quella del dirottamento degli indirizzi IP non è facilmente aggirabile dagli utenti di Internet, se non ricorrendo, a esempio, alle cosiddette connessioni private virtuali (VPN, *virtual private network*) stabilite verso fornitori esteri (peraltro sovente a titolo oneroso) che, a quel punto, sarebbero in grado di far approdare il nostro computer alla destinazione altrimenti inibita (illegale). Un *escamotage* che funziona a patto che le VPN non vengano intercettate e bloccate (come può succedere invece nella Repubblica Popolare Cinese[23]).

# Campione utilizzato

L'indagine è stata effettuata elaborando i dati emersi da un questionario sottoposto, nel mese di dicembre 2015, agli operatori ICT della pubblica amministrazione attraverso diversi canali: gruppi di Facebook con interesse

[20] A. Toonk, *Turkey Hijacking IP addresses for popular Global DNS providers*: http://www.bgpmon.net/turkey-hijacking-ip-addresses-for-popular-global-dns-providers/

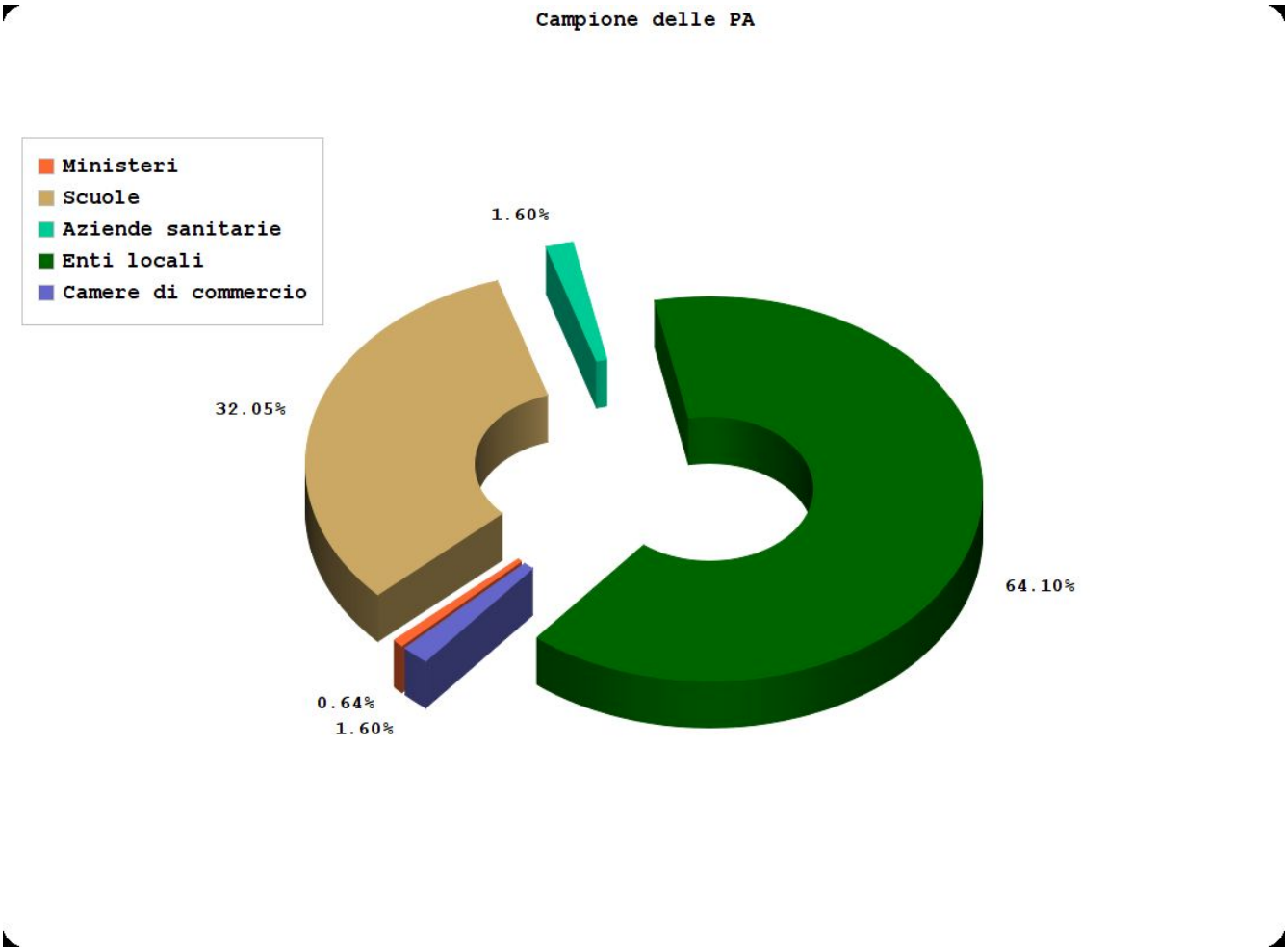
[21] G. Scorza, *Caso Vajont.info: il provvedimento di sequestro*: http://www.leggioggi.it/2012/02/19/esclusiva-caso-vajont-info-il-provvedimento-di-sequestro/

[22] R. Fielding, J. Reschke, *Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing*: https://www.rfc-editor.org/rfc/rfc7230.txt

[23] J. Russel, *China Continues Its Crackdown On VPN Services:* http://techcrunch.com/2015/09/07/china-continues-its-crackdown-on-vpn-services/

nella Pubblica amministrazione, associazione dei cosiddetti "*digital champions*" italiani[24], comunità degli addetti informatici della P.A.[25], vari forum di interesse per i dipendenti pubblici.

Ne è scaturita una cospicua (oltre cinquecento soggetti) e inaspettata, seppur volontaria, partecipazione che, proprio per questo, ha reso il **campione sufficientemente diversificato** in grado di presentare risposte provenienti da enti locali, scuole, aziende sanitarie, ministeri e camere di commercio.




A ogni modo, visto l'esito dell'elaborazione (illustrato sotto), a garanzia dell'anonimato degli intervenuti e avendo voluto esaudire il desiderio di alcuni ignoti partecipanti, i dati (sorgente) dell'indagine sono stati tutti distrutti.

## Struttura del questionario

[24] Digital Champions, http://www.digitalchampions.it

[25] Opensipa, *La Comunità e l'Associazione dei Sistemisti Informatici della Pubblica Amministrazione*: http://www.opensipa.it

L'indagine si è basata su **ventisei domande** ciascuna delle quali necessitava una azione da compiere su un calcolatore appartenente alla rete interna dell'ente pubblico secondo il seguente algoritmo d'esempio:

```
DATE=`date -u +%Y%m%d%H%M%S`
IP=`curl -s whatismyip.akamai.com`
NS=`dig whoami.akamai.net +short`
LEA1=`dig www.banqueoption.com +short`
GLEA1=`dig www.banqueoption.com @8.8.8.8 +short`
CLEA1=`dig www.banqueoption.com @208.67.222.222 +short`
LEA1HTTP=`nc -w 5 -z www.banqueoption.com 80`
AAMS1=`dig expect.at +short`
GAAMS1=`dig expect.at @8.8.8.8 +short`
CAAMS1=`dig expect.at @208.67.222.222 +short`
AAMS1HTTP=`nc -w 5 -z expect.at 80`
```

Innanzitutto occorreva indicare con quale indirizzo IP ci si presenta su Internet, poi quale server DNS si utilizza per risolvere i nomi a dominio.

Seguiva una serie di questioni sulla capacità, del calcolatore utilizzato, di visualizzare le pagine di determinati nomi a dominio sottoposti a censura.

Dall'elenco sono state volutamente escluse risorse appartenenti alla *black list* del CNCPO che è destinata esclusivamente[26] agli operatori di rete così come sono definiti dal codice delle comunicazioni elettroniche[27].

Il questionario si concludeva con un campo opzionale per poter esprimere liberamente un commento sull'indagine.

---

[26] Il Codice delle comunicazioni elettroniche è chiaro riguardo l'esclusività dell'accesso alle *black list* del CNCPO da parte degli operatori di rete. Ritengo tuttavia di poter riconoscere un *vulnus* nei confronti del soggetto che, pur essendosi qualificato presso il RIR (*regional internet registry*) di riferimento in Italia (RIPE NCC), per l'assegnazione di un numero di sistema autonomo e risorse IP, non sia compreso nella definizione dell'articolato.

Caso emblematico è quello di una Pubblica amministrazione che, fermo restando il divieto dell'articolo 6 della norma citata, sia assegnataria di risorse numeriche (AS e IP) ma che, non compresa nella definizione legislativa, sia impedita di accedere alle liste del CNCPO (salvo eccezionale lasciapassare scritto dal Ministero dello Sviluppo economico al Dipartimento di Pubblica sicurezza).

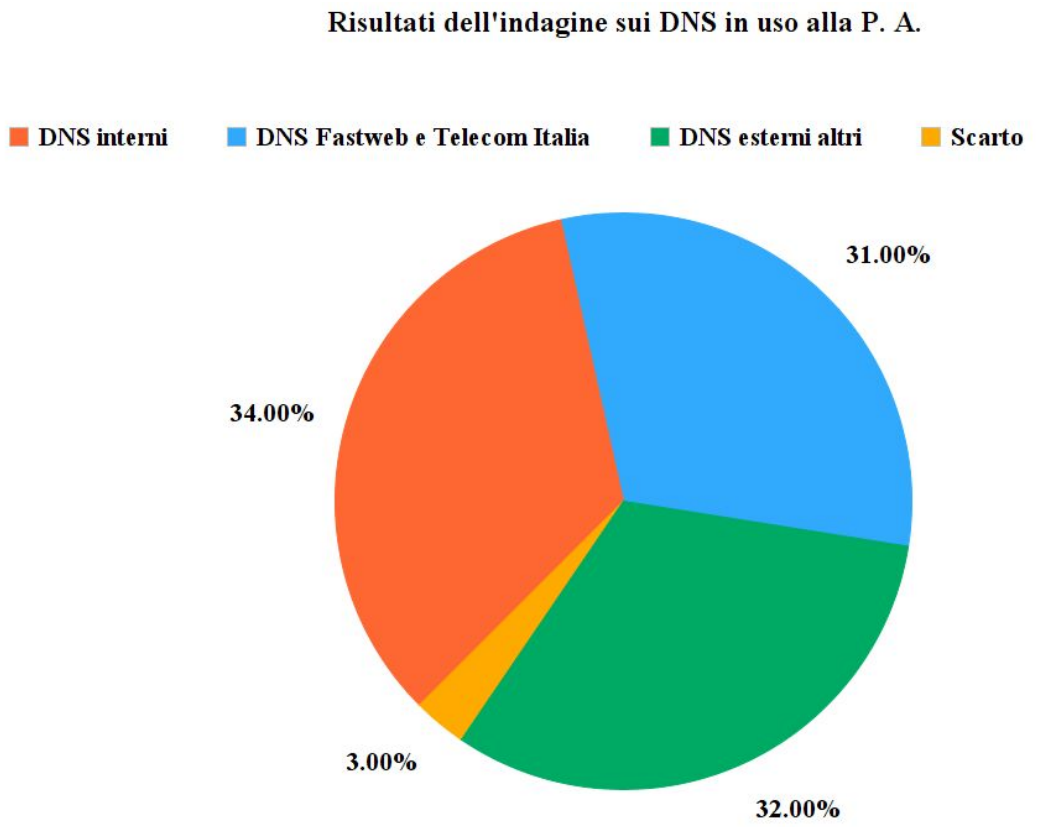
La fattispecie sarebbe dunque da rivedere nell'ottica di una più ampia definizione di "operatore di rete" che dovrebbe annoverare anche quei soggetti che, pur non essendo OTAG (operatore di telecomunicazioni con autorizzazione generale), siano però titolari di un sistema autonomo.

[27] Ordinamento italiano, *Codice delle comunicazioni elettroniche*: http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2003-08-01;259

# Risultati ottenuti

Le risposte sono state quasi tutte coerenti (giusto il 3% infatti non è stato preso in considerazione) e hanno sorprendentemente rivelato la presenza di **scenari piuttosto preoccupanti**.

Solo il 23% di chi ha risposto dimostra una soddisfacente aderenza al rispetto delle prescrizioni precedentemente illustrate.




Il restante 66% ha messo in luce un contesto disastroso popolato di inadeguatezze all'osservanza delle cogenti previsioni dell'ordinamento italiano in materia di contrasto all'illegalità in genere sulla rete Internet.

L'analisi ha comunque consentito di individuare, tra tutti i dati ricevuti in fase di indagine, tre ampi raggruppamenti (qui sotto elencati) a seconda delle impostazioni dichiarate dei server DNS, dell'indirizzo IP di navigazione e della capacità di contattare e visualizzare determinati contenuti rispondenti ad alcuni nomi a dominio scelti a caso da tre distinte *black list*.

## Enti che usano DNS interni

Il 34% delle risposte ottenute evidenzia il ricorso a server DNS interni all'infrastruttura informatica dell'ente pubblico ed erroneamente gestito.

Per server interno intendo un servizio che, conoscendo l'indirizzo di almeno uno dei tredici *root server*[28], sia per questo in grado di risalire automaticamente a qualsiasi server DNS autoritativo e di contattarlo per ottenere risposte circa gli abbinamenti tra nomi a dominio e indirizzi IP.

Una delle peggiori fattispecie possibili: uso di risolutori di nomi a dominio interni che non tengono conto di alcuna *black list* tra quelle indicate dalle norme (oltre a ulteriori criticità più avanti dettagliate).

## Enti che usano DNS esterni di Telecom Italia e Fastweb

Il 31% delle risposte ottenute rivela l'**uso corretto** (e presumibilmente efficiente anche dal punto di vista delle *performance*) dei server DNS forniti dagli operatori di rete individuati nella vigente convenzione CONSIP[29] e che erogano la connettività alle P.A. in questione.

Le *black list* formate dalle norme vengono generalmente onorate e, nei rari casi in cui non fossero tempestivamente aggiornate, la responsabilità non sarebbe certo da attribuire ai dirigenti pubblici.

## Enti che usano altri DNS esterni

Il 32% delle risposte dimostra l'uso di server DNS resi disponibili da piccoli fornitori (fuori da convenzione CONSIP, come a esempio potrebbero essere dei consorzi di comuni o delle società private partecipate dal pubblico o alcuni OTAG, operatore di telecomunicazioni con autorizzazione generale[30]) o da società estere come:

Google Public DNS[31] (IPv4 8.8.8.8 e 8.8.4.4; IPv6 2001:4860:4860::8888 e 2001:4860:4860::8844);

Cisco OpenDNS[32] (IPv4 208.67.222.222 e 208.67.220.220; IPv6 2620:0:ccc::2 e 2620:0:ccd::2).

Stando ai dati raccolti, i server dei piccoli operatori di rete quasi mai rispetterebbero le inibizioni imposte dalle norme, così come i server di risoluzione dei nomi messi a disposizione gratuitamente dalle società estere menzionate.

---

[28] Root Server Technical Operations Assn: http://www.root-servers.org/

[29] CONSIP, *Servizi di connettività nell'ambito del Sistema Pubblico di Connettività (SPC) per le Pubbliche Amministrazioni*: http://www.consip.it/news_ed_eventi/2013/10/notizia_0015

[30] Ministero dello Sviluppo economico, *Autorizzazioni e licenze nel settore delle comunicazioni elettroniche*: http://www.sviluppoeconomico.gov.it/index.php/it/comunicazioni/servizi-alle-imprese/autorizzazioni-e-licenze

[31] Google, *Public DNS*: https://developers.google.com/speed/public-dns

[32] Cisco, *OpenDNS*: https://www.opendns.com

Anzi, quest'ultimo caso, nonostante i benefici circa la sicurezza pubblicizzati da entrambi i servizi citati[33], può senz'altro essere classificato come una **scelta superficiale**, per usare un eufemismo, nella prospettiva di ottemperare alle prescrizioni normative.

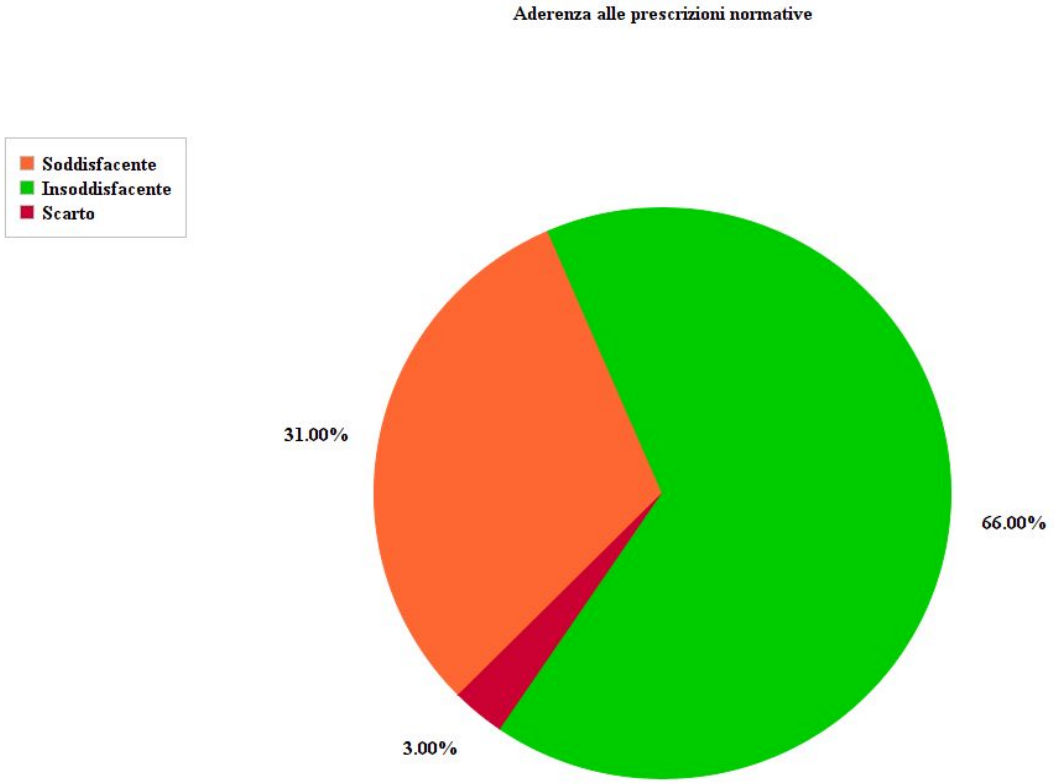
Seppure infatti il mercato proponga servizi a pagamento di risoluzione dei nomi programmati per proteggere gli utenti da siti web che diffondono subdolamente programmi non desiderati se non addirittura nocivi o da siti web dal contenuto classificato come offensivo, sarà improbabile reperire all'estero una offerta preconfezionata tagliata su un profilo che soddisfi pienamente quanto statuito dalle leggi italiane (almeno sino a oggi).

Inoltre, come palesemente risultato dall'indagine (nello spazio riservato ai commenti facoltativi), non si può escludere l'esistenza, tra i piccoli operatori di rete fornitori di alcune P.A., di server DNS appartenenti agli operatori stessi ma che svolgono semplicemente una funzione di inoltro verso servizi esteri di risoluzione dei nomi.

Si tratta di una **pratica scorretta** per molteplici ragioni tra le quali basterà nominare la palese inosservanza delle norme per apprezzare pienamente la scarsa serietà del servizio offerto.

[33] Google, *Security Benefits*: https://developers.google.com/speed/public-dns/docs/security

Cisco, *Home Internet Security*: https://www.opendns.com/home-internet-security/




# Ulteriori criticità rilevate

In modo del tutto incidentale sono emerse, a carico del 25% dei server DNS dichiarati (esclusivamente appartenenti al gruppo “DNS interni” e al gruppo “altri DNS esterni”), alcune criticità facilmente individuabili sotto il profilo della sicurezza, in senso stretto, dei dèmoni deputati all’erogazione del servizio di risoluzione dei nomi (o a carico della loro configurazione e gestione).

Sottolineo che si tratta di problemi che comunemente affliggono i servizi pubblicati su Internet nella sua globalità. [34]

La questione diventa però meritevole di scrupolosa attenzione allorquando coinvolga servizi pubblici, affinché lo Stato funzioni, considerate le ambizioni del Codice dell’amministrazione digitale.[35]

[34] The Measurement Factory, *Number of known open resolvers for each autonomous system:* http://dns.measurement-factory.com/surveys/openresolvers/ASN-reports/latest.html

[35] Ordinamento italiano, *Decreto legislativo 82 del 7 marzo 2005*: http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2005-03-07;82!vig=

### Problemi di sicurezza dei DNS interni e dei DNS esterni di piccoli ISP

Alcuni server analizzati sono gravemente esposti a chiunque per qualunque richiesta (tecnicamente sono classificabili come *open resolver*[36]).

Altri invece, sebbene non *open resolver*, rispondono alle *query* di chiunque per le zone di cui sono anche autoritativi ignorando una delle più note (e antiche[37]) raccomandazioni di buona pratica nella gestione dei server di risoluzione dei nomi a dominio: **distinguere e segregare** le specialità del DNS (funzione autoritativa, di *cache*, ricorsiva, di inoltro)[38].

Entrambe le criticità rilevate sono pericolose perché potrebbero dare man forte negli attacchi di tipo *denial of service*, cioè interruzione di servizio (DoS, *denial of service* e DDoS, *distributed denial of service*), rendendo i server interessati dei veri e propri strumenti per l'amplificazione[39] di eventuali azioni criminose.

Eventi che, sempre più spesso, si registrano nel mondo e che guadagnano pagine di cronaca nelle riviste specializzate come recentemente accaduto in Turchia.[40]

## Possibili soluzioni

Il quadro emerso dalle spontanee partecipazioni alla rilevazione oggetto di questa analisi è a fosche tinte.

[36] D. Wessels, *Mitigating DNS Denial of Service Attacks*: https://www.dns-oarc.net/wiki/mitigating-dns-denial-of-service-attacks

[37] D. Wessels, *Running An Authoritative-Only BIND Nameserver*: https://ftp.isc.org/isc/pubs/tn/isc-tn-2002-2.html

[38] A. Cezar, *Securing DNS Servers*: http://blog.isc2.org/isc2_blog/2008/08/securing-dns-se.html

[39] M. Prince, *Deep Inside a DNS Amplification DDoS Attack*: https://blog.cloudflare.com/deep-inside-a-dns-amplification-ddos-attack/

[40] E. Sozeri, *Turkish Internet hit with massive DDoS attack:* http://www.dailydot.com/politics/turkey-ddos-attack-tk-universities/

La disorganizzazione del peculiare àmbito trattato appare endemica[41] come frutto di un coordinamento latitante sia degli alti livelli della dirigenza dello Stato sia degli organismi preposti alla guida e alla regolamentazione anche di questi aspetti dell'Italia digitale.

È forse appena il caso di ribadire qui il ruolo centrale e determinante del DNS nel corretto funzionamento della rete Internet anche per l'applicazione delle inibizioni che la norma italiana in questo momento storico impone.

Non può e anzi non deve dunque essere un servizio delegato a una gestione locale della singola Pubblica amministrazione (DNS interni) né lasciato in balìa della discrezionalità degli operatori ICT degli enti che, a volte per imperizia, a volte per comodità esternalizzano il servizio (DNS esterni) anche a fornitori che non sono tenuti a osservare le norme italiane (DNS pubblici all'estero).

Posto che la Pubblica Amministrazione debba attingere ai servizi di connettività disponibili in apposite convenzioni tra CONSIP e gli operatori di rete, occorre pensare a una gestione centralizzata del servizio DNS articolato sul territorio con la presenza di istanze replicate in ANYCAST[42] e reso disponibile e obbligatorio per tutte le strutture pubbliche (salvo eventualmente il caso di una P.A. che sia titolare di un sistema autonomo[43]).

In questo modo si conseguirebbero facilmente obiettivi importanti come sicurezza, robustezza, affidabilità, tempismo.

Quanto al momento di produzione e diffusione delle *black list* sono persuaso che sia necessaria la costituzione, in seno per esempio ad AgID[44] (Agenzia per l'Italia digitale) visto il suo statuto[45], di un **punto unico di accesso** per gli operatori di rete (secondo la più ampia definizione proposta in nota 26).

Cioè per facilitare, normalizzare e livellare l'applicazione delle inibizioni che lo Stato impone agli *Internet Service Provider* (e non solo), tutti gli attori coinvolti (CNCPO, ADM, AGCOM, Autorità giudiziaria) dovrebbero essere coordinati nei formati da utilizzare, nei tempi di aggiornamento (aggiunta e rimozione delle voci).

---

[41] A. Prado, articoli con tag Public Administration:

*Analysis on poor reputation of the italian Public Administration websites*

*Reverse DNS lookup for Italian Government's mail exchangers*

*HTTPS Zombies among Italian Public Administration's web sites*

*Where do italian Public Administration web sites live?*

*DNSSEC, unidentified flying object in the sky over italian Public Administration*

*Italian Public Administration web sites (in)security: 2014 report*

*Anti spam measures adopted by italian Public Administrations: mostly SPF*

*IPv6 in the Internet resources of italian Public Administration at a glance*

https://www.prado.it/tag/public-administration/

[42] J. Abley, K. Lindqvist, *Operation of Anycast Services*: https://www.rfc-editor.org/rfc/rfc4786.txt

[43] RIPE NCC, *Local Internet Registries offering service in Italy*: https://www.ripe.net/membership/indices/IT.html

[44] Agenzia per l'Italia digitale: http://www.agid.gov.it/

[45] AgID, *Pubblicato in Gazzetta Ufficiale lo statuto dell'AgID*: http://www.agid.gov.it/notizie/2014/02/14/pubblicato-gazzetta-ufficiale-lo-statuto-dellagid

Penso che lo Stato potrebbe facilitare l'**auto-valutazione della conformità** alle norme di inibizione così da poter diffondere una corretta consapevolezza della questione, sia agli operatori ICT in servizio presso la Pubblica Amministrazione, sia alle aziende, sia ai privati.

Dovrebbe per questo realizzare uno strumento (anche una semplice APP web), accessibile da chiunque su Internet, che servirebbe anche per verificare la corretta e tempestiva applicazione delle *black list* attraverso reali connessioni a nomi a dominio di test appositamente inseriti negli elenchi.

Infine, finché permarranno disposizioni di censura emanate da più nazioni dell'Unione europea[46], auspico un **coordinamento transnazionale** per l'applicazione dei criteri di restrizione nella navigazione delle pubbliche amministrazioni dei Paesi coinvolti.

[46] Freedom House, *Freedom on the NET 2015*: https://freedomhouse.org/report/freedom-net/freedom-net-2015