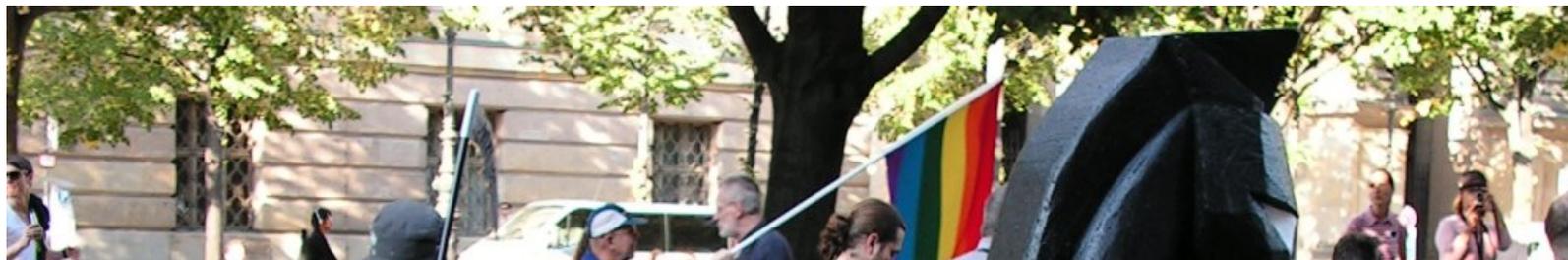




Più trojan per tutti: le diverse modalità di utilizzo dei "captatori informatici", tra giurisprudenza e progetti di legge

Avv. Giovanni Battista GALLUS, LL.M., Ph.D - gallus@array.eu

*Hermes Center for Transparency and Digital Human Rights
Nexa Center for Internet and Society*



- Captatori 2.0
- Effetti collaterali della raccolta di 0 day
- Il framework EU
- DDL (oramai legge) Orlando e captatori



Photo by Leralle



A LONG TIME AGO
IN A GALAXY FAR
FAR AWAY

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



Trojans and Backdoors for investigative purposes and fundamental rights and freedoms: is it possible to find a balance?

Avv. Giovanni Battista GALLUS, LL.M., Ph.D - gallus@array.eu

*Hermes Center for Transparency and Digital Human Rights
Nexa Center for Internet and Society*

Avv. Giovanni Battista Gallus  @gbgallus



Thorny issue: State shopping for 0 days and vulnerabilities

L'anno scorso, a un altro convegno

Avv. Giovanni Battista Gallus  @gbgallus

The NSA reportedly believes North Korea was responsible for WannaCry ransomware attacks

by Jacob Kastrenakes | Jun 14, 2017, 8:29pm EDT

SHARE TWEET LINKEDIN



Image: SecureList / AO Kaspersky Lab

North Korea increasingly appears to have been behind the ransomware attack that [infected hundreds of thousands of computers](#) last month and [shut down](#) hospitals, businesses, and other systems in the process.

17

Technology

NSA officials worried about the day its potent hacking tool would get loose. Then it did.

The National Security Agency campus in Fort Meade, Md. (2013 photo by Patrick Semansky/AP)

By Ellen Nakashima and Craig Timberg May 16

When the National Security Agency began using a new hacking tool called EternalBlue, those entrusted with deploying it marveled at both its uncommon power and the widespread havoc it could wreak if it ever got loose.

Some officials even discussed whether the flaw was so dangerous they should reveal it to Microsoft, the company whose software the government was exploiting, according to former NSA employees who spoke on the condition of anonymity given the sensitivity of the issue.

But for more than five years, the NSA kept using it — through a time period that has seen several serious security breaches — and now the officials' worst fears have been realized. The malicious code at the heart of the WannaCry virus that hit computer systems globally late last week was apparently stolen from the NSA, repackaged by cybercriminals and unleashed on the world for a cyberattack that now ranks as among the

EU Policy Framework



- Constitutional Affairs
- Justice, Freedom and Security
- Gender Equality
- Legal and Parliamentary Affairs
- Petitions

Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices

STUDY FOR THE LIBE COMMITTEE

EN

2017



Policy proposals Fundamental rights and privacy

Resolution on Privacy Impact Assessment, focused on necessity and proportionality + input from Data Protection Authority

Clear and precise legal basis

Research, evaluation and monitoring

EU Agency for Fundamental Rights (FRA) to develop a **practitioner handbook** related to the governing of hacking by law enforcement.

Proper training for judiciary and data protection authorities

Policy proposals Security of the Internet

Resolution on Impact Assessment to examine the impact of new or existing State hacking laws on the security of the Internet

Commitment to strong encryption & no backdoors

Develop appropriate responses to handling zero-day vulnerabilities

The handbook should cover the risks posed to the security of the Internet by using hacking techniques.

Encourage debate (including law enforcement agents)

TROJAN HORSES
FOR THE COMMON GOOD
HANDBOOK
FOR LAW ENFORCERS



Da noi

La manovra è legge: ok del Senato alla fiducia con 144 sì

Pensioni, ecco la nuova platea della quattordicesima

Alitalia: Calenda, i commissari stanno lavorando bene

Quinta fumata nera per il nuovo giudice, Consulta senza...

IL DDL APPROVATO CON 267 SÌ

Riforma processo penale, ok definitivo della Camera

di A. Gagliardi e V. Nuti | 14 giugno 2017



Via libera definitiva della Camera al disegno di legge di modifica del codice penale e del codice di procedura penale. I voti favorevoli sono

Atti Parlamentari - 1 - Camera dei Deputati
XVII LEGISLATURA - DISEGNI DI LEGGE E RELAZIONI - DOCUMENTI

CAMERA DEI DEPUTATI N. 4368

DISEGNO DI LEGGE

PRESENTATO DAL MINISTRO DELLA GIUSTIZIA (ORLANDO)

DI CONCERTO CON IL MINISTRO DELL'INTERNO (ALFANO)

E CON IL MINISTRO DELL'ECONOMIA E DELLE FINANZE (PADOAN)

approvato dalla Camera dei deputati il 23 settembre 2015 (v. stampato Senato n. 2067)

E

PROPOSTE DI LEGGE

D'INIZIATIVA DEI DEPUTATI

FERRANTI, VERINI, MATTIELLO, GIULIANI, MARZANO, BAZOLI, CAMPANA, TARTAGLIONE

approvata dalla Camera dei deputati il 24 marzo 2015 (v. stampato Senato n. 1844)

MOLTENI, ALLASIA, ATTAGUILE, BORGHESI, MATTEO BRAGANTINI, BUSIN, CAON, CAPARINI, GRIMOLDI, MARCOLIN, GIANLUCA PINI

approvata dalla Camera dei deputati il 29 luglio 2015 (v. stampato Senato n. 2032)



Punti essenziali

- Decreto legislativo entro tre mesi
- Regola solo l'attivazione remota del microfono
- Si applica esclusivamente alle “intercettazioni di comunicazioni o conversazioni tra presenti mediante immissione di captatori informatici in dispositivi elettronici portatili”

What about IoH[acked]T[hings]?

THE VERGE

TECH SCIENCE CULTURE CARS REVIEWS LONGFORM VIDEO MORE



US & WORLD TECH CYBERSECURITY

The CIA is hacking Samsung Smart TVs, according to WikiLeaks docs

88

by Russell Brandom | @russellbrandom | Mar 7, 2017, 10:14am EST

SHARE TWEET LINKEDIN



Photo by Olivier Doulier - Pool/Getty Images

SECTIONS SEARCH

Los Angeles Times

SUBSCRIBE SALE: 12 wks / 99¢

LOG IN

FRIDAY JUN. 16, 2017

LOCAL SPORTS POLITICS ENTERTAINMENT OPINION MOST POPULAR PLACE AN AD



BUSINESS / Michael Hiltzik

Column Apple, the FBI, and the Internet of Things: Your whole house is open to attack



oatpixel.com...

gress on Tuesday about the issues in his encryption fight with Apple.



Il perimetro di applicabilità

- Senza limiti per i reati di cui all'art. 51, commi 3-bis e 3-quater, del c.p.p. (ipotesi più gravi di crimine organizzato e terrorismo)
- Per gli altri reati, nei limiti dell'art. 266, comma 1, c.p.p., nei luoghi di cui all'articolo 614 del codice penale soltanto qualora ivi si stia svolgendo l'attività criminosa
- 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;
- Possibili anche con decreto del PM (per i reati più gravi), ove ricorrano concreti casi di urgenza

Le procedure di registrazione

- l'attivazione del microfono 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;
- la registrazione audio deve essere avviata dalla polizia giudiziaria o dagli ausiliari di PG su indicazione della polizia giudiziaria
- Nessun esplicito obbligo di logging, salva l'ora di inizio e fine della registrazione,
- Le registrazioni devono essere trasferite soltanto verso il server della procura **così da garantire originalità e integrità delle registrazioni;**
- Al termine della registrazione il captatore informatico deve essere disattivato e reso definitivamente inutilizzabile su indicazione del personale di PG

Le procedure di registrazione

Marescia' che faccio, avvio?



L'utilizzo delle captazioni

- 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 per cui è previsto l'arresto obbligatorio in flagranza (art. 380 c.p.p.);
- 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;



- Devono essere utilizzati soltanto programmi informatici conformi a requisiti tecnici stabiliti con decreto ministeriale 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

Trojan d'
Origine
Controllata

Photo by Leralle



~~PRIVACY~~
~~INTERNATIONAL~~

In Advance of a Parliamentary Consultative
Process

- ---

**Privacy International's
Analysis of the Italian
Hacking Reform, under DDL
Orlando**



Cosa manca?

Nessuna regolamentazione per perquisizioni / keylogging / GPS monitoring / Video recording

Utilizzabili per molteplici reati

Nessuna prescrizione obbligatoria sul logging

Le attività sono eseguibili dagli ausiliari di PG

Mancanza di trasparenza e controllo

Nessuna normazione sulle vulnerabilità

Siamo in
buona
compagnia

[Home](#) / [News](#) /

'State trojans': New German law enables police to hack into encrypted messengers

Published time: 23 Jun, 2017 10:37

Edited time: 23 Jun, 2017 11:30

[Get short URL](#)



German police may now hack into messengers like WhatsApp using "state trojans" to intercept user communications before they are encrypted on their devices, according to a new law swiftly passed by the parliament.

The new legislation allows police investigators to use a "state trojan" to hack into a suspect's mobile device, tablet, or computer, and get full access to their chat messages, video recordings, or other private data, German media reported.

[Read more](#)

The "state trojans" could make it easier to bypass the encryption employed by popular messaging services, including WhatsApp, as

Un male necessario?

"Democratic societies nowadays find themselves threatened by **highly sophisticated forms of espionage** and **by terrorism**, with the result that **the State must be able, in order effectively to counter such threats**, to undertake the secret surveillance of subversive elements operating within its jurisdiction.

The Court has therefore to accept that the **existence of some legislation granting powers of secret surveillance over the mail, post and telecommunications is, under exceptional conditions, necessary in a democratic society** in the interests of national security and/or for the prevention of disorder or crime."

Distruggere la democrazia con il pretesto di difenderla?

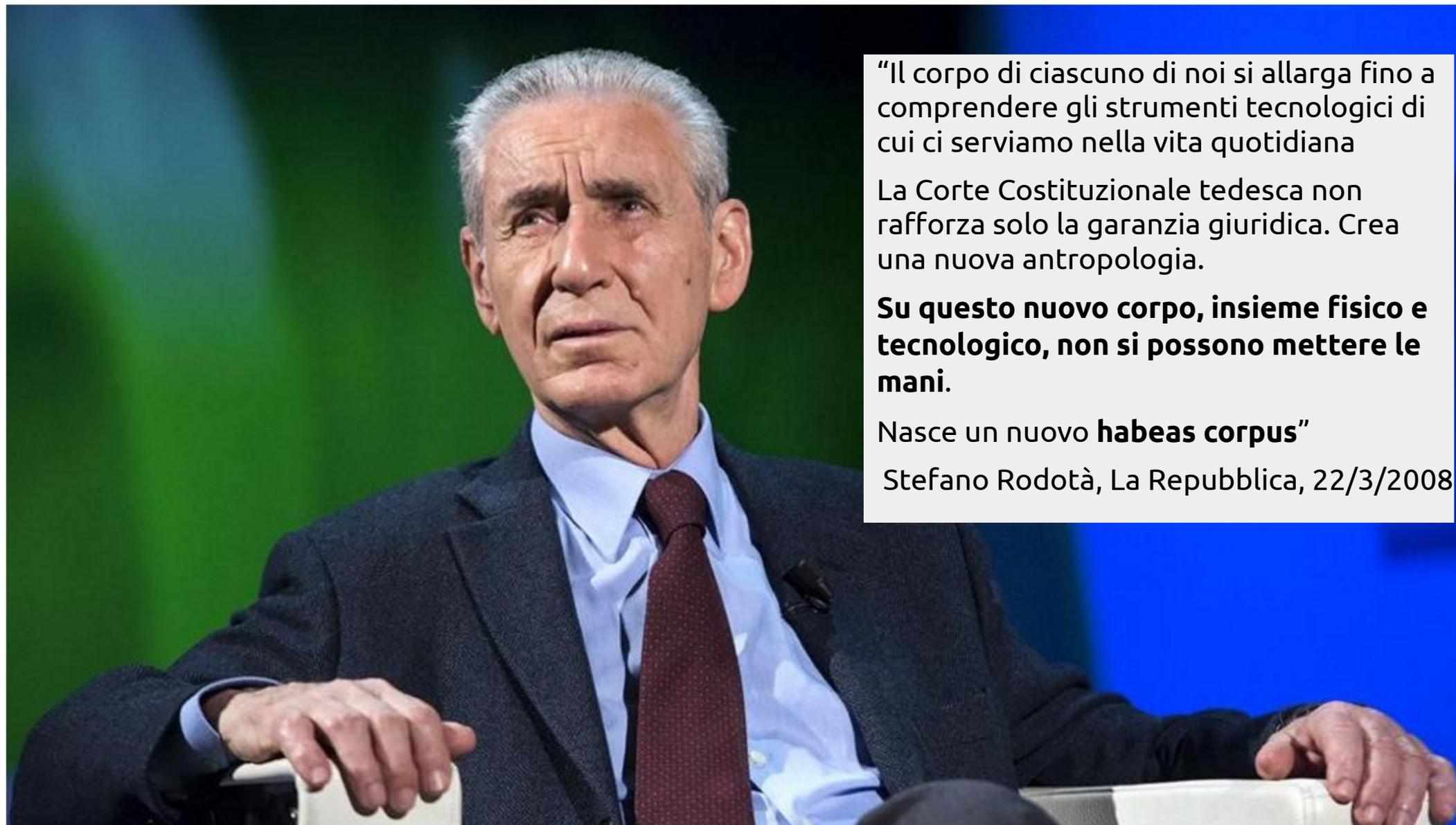
"Nevertheless, the Court stresses that this does not mean that the Contracting States enjoy an **unlimited discretion to subject persons within their jurisdiction to secret surveillance.**

The Court, being aware of the danger such a law poses of **undermining** or even **destroying democracy on the ground of defending it**, affirms that the **Contracting States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate.**"

E.C.H.R.

Klass vs Germany
6 September 1978

Grazie Stefano Rodotà



“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.

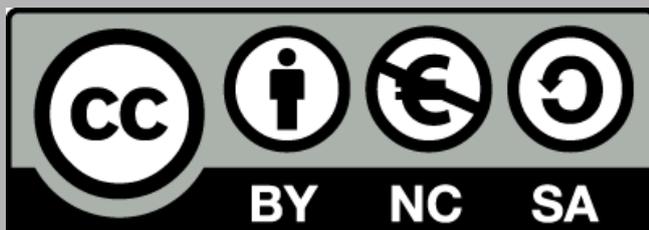
Nasce un nuovo **habeas corpus**”

Stefano Rodotà, La Repubblica, 22/3/2008

Foto La Stampa LAPRESSE

Domande?





Unless stated otherwise,
all texts are distributed
under a Creative Commons
Attribution – non
commercial – sharealike
3.0 Unported license

Thank you

Avv. Giovanni Battista Gallus

gallus@array.eu  @gbgallus