Il Datagate ed i limiti del diritto

e-privacy 2013
winter edition
Milano, Università Bocconi, 15-16 novembre 2013

Dalle rivelazioni di Snowden:

- ☐ PRISM: dati raccolti in upstream collection e mediante accesso ai server degli ISP
- ☐ TEMPORA: dati raccolti in upstream collection sui cavi a fibra ottica che arrivano in UK

NSA

Government Communications Headquarters

Gli U.S.A. hanno respinto le accuse sostenendo di aver agito conformemente a quanto stabilito dal FISA (Foreign Intelligence Surveillance Act) emanato nel 1978 (ed emendato dopo l'11.09.2001) per tutelare gli americani dopo lo scandalo Watergate ed evitare l'abuso interno fatto da Nixon dei servizi di intelligence

Il Governo UK, da parte sua, sostiene di aver agito legittimamente in base a quanto stabilito dal RIPA (Regulation of Investigatory Power Act) del 2000, un atto che regola intercettazioni, acquisizione di metadati comunicativi e sorveglianza elettronica nel Regno Unito

Sezione 702 FISA
(50 U.S.C. § 1801)

- ☐ Prevede la possibilità di sorvegliare elettronicamente persone straniere (i.e. non cittadini americani) situate all'estero (fuori U.S.A.) per acquisire foreign intelligence information

- ☐ f.i.i. include qualsiasi informazione di interesse per la sicurezza nazionale in relazione a potenziali attacchi di paesi stranieri, sabotaggi, terrorismo internazionale, antispionaggio, nonché informazioni relative ad un foreign power (governi, istituzioni e organizzazioni politiche straniere, ma anche gruppi terroristici)

Sezione 702 FISA
(50 U.S.C. § 1802)

- ☐ Il Presidente può autorizzare la sorveglianza elettronica senza un ordine della Corte per il periodo di 1 anno se l'Attorney General certifica che si tratta di attività diretta a:

  - acquisire il contenuto di comunicazioni trasmesse da mezzi di comunicazione usati esclusivamente da e fra foreign powers

  - sempre che non vi sia nessuna concreta probabilità che la sorveglianza possa portare ad acquisire il contenuto di una conversazione di cui è parte un cittadino americano

Sezione 702 FISA (50 U.S.C. § 1804)

- La sorveglianza elettronica può essere disposta anche in forza di un **Court order**

- In questo caso la richiesta necessita di una **probable cause** sul fatto che l'obiettivo della sorveglianza sia un foreign power o un agente di un foreign power e che le strutture o i luoghi a cui la sorveglianza è diretta siano usati, o stiano per essere usati, da un foreign power o da un agente di un foreign power

Sezione 702 FISA
(50 U.S.C. § 1881)

- L'Attorney General e il Direttore dell'NSA possono congiuntamente autorizzare, per il periodo di 1 anno, il monitoraggio di persone (non cittadini americani) ragionevolmente situate fuori dal territorio U.S.A. al fine di acquisire foreign intelligence information

- La sorveglianza necessita di una certification diretta alla FISA Court, oppure di una determination, nei casi urgenti

RIPA §8(1) e 8(2)

1. Quando si tratta di internal communication (i.e. non inviate né ricevute al di fuori delle British Islands) le intercettazioni sono autorizzate con un warrant che deve indicare:
   la specifica persona da monitorare, ovvero
   gli specifici presupposti in relazione ai quali il warrant viene richiesto

2. Il warrant deve contenere indirizzi, numeri, strumenti e ogni altro elemento utilizzato per identificare le comunicazioni che devono essere intercettate

RIPA §8(4)

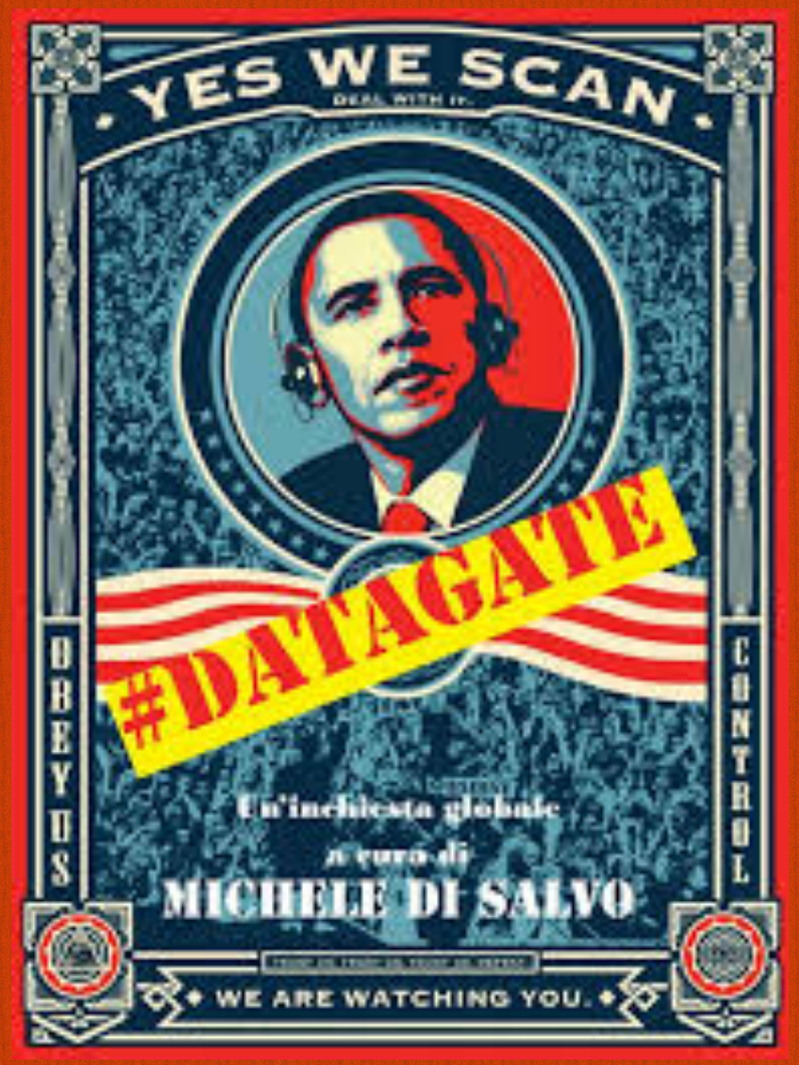
Quando si tratta di external communication (i.e. inviate o ricevute al di fuori delle British Islands) il warrant è generico in quanto non si applicano le disposizioni precedenti:
non è quindi necessario identificare una persona specifica come oggetto di intercettazione, né è necessario indicare un particolare indirizzo, numero o strumento quale oggetto di intercettazione, essendo sufficiente "the descriptions of intercepted material the examination of which he considers necessary"

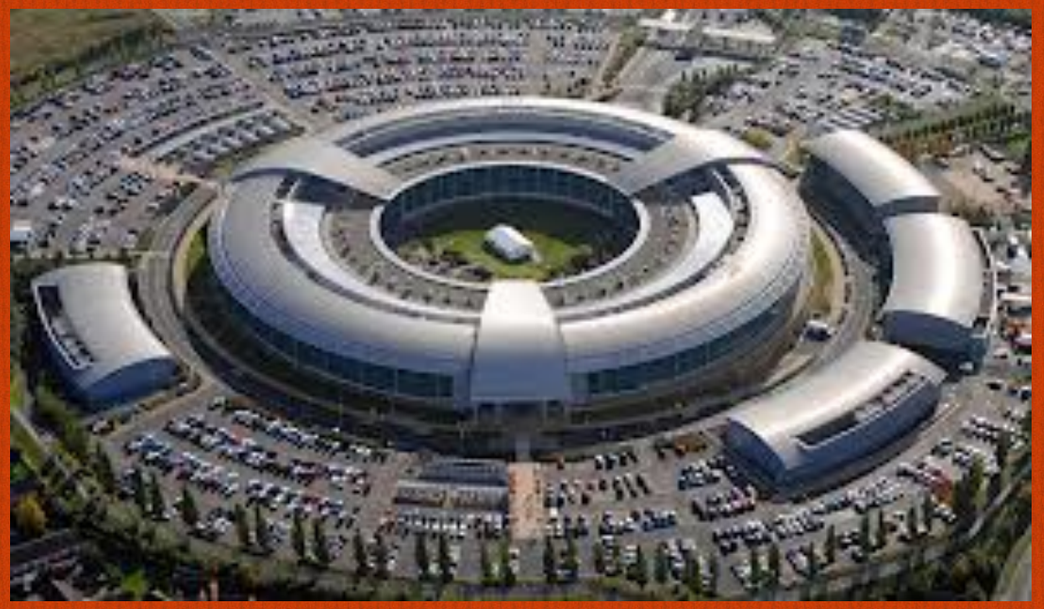
USA		UK	
La legge tutela gli americani	NON tutela gli stranieri	La legge tutela comunicazioni interne	NON tutela le comunicazioni esterne

In entrambi i casi siamo di fronte a disposizioni legislative basate su principi tradizionali del diritto:

1. **territorialità**

2. **tutela di diritti fondamentali quali libertà di comunicazione e di espressione**


YES WE SCAN
#DATAGATE
OBEY US
CONTROL
Un'inchiesta globale
a cura di
MICHELE DI SALVO
WE ARE WATCHING YOU.



La condivisione di dati tra agenzie di intelligence consente di bypassare i limiti del diritto nazionale

Perché oggi è diverso da ieri

- ☐ le comunicazioni sono globalizzate
- ☐ la tecnologia consente di raccogliere agevolmente una grande quantità di dati
- ☐ le tecniche di analisi dei big data consentono di elaborare frazioni minimissime ed eterogenee di dati o metadati di comunicazione

Anche le reazioni sono state tradizionali, come si trattasse della solita, vecchia intelligence

REAZIONI POLITICHE (cfr. Brasile)

REAZIONI FISICHE (infrastrutture e localizzazione data center)

Privacy International UK ha intentato una causa contro il Governo britannico

Per violazione dell'art.8 della CEDU

Art.8 CEDU

- Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza.

- Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui

- ☐ Le conversazioni telefoniche e quelle di posta elettronica rientrano nel concetto di corrispondenza
- ☐ La cronologia di una ricerca web ed i metadati di una comunicazione elettronica rientrano nel concetto di vita privata
- ☐ Nella causa Weber v. Germany (2006), la Corte EDU ha stabilito che per sostenere la violazione dell'art.8 non occorre la prova che le comunicazioni del ricorrente siano state effettivamente monitorate, essendo sufficiente che potenzialmente possano essere state oggetto di sorveglianza

- La giurisprudenza della Corte EDU sul concetto di ingerenza nella vita privata autorizzata per legge è copiosa

- La legge deve essere **accessibile**, nel senso che deve indicare "con ragionevole chiarezza il campo di applicazione e le modalità di esercizio del potere discrezionale attribuito alle pubbliche autorità"

- La legge deve essere **prevedibile**, il che non significa che il cittadino debba essere in grado di prevedere quando sarà sorvegliato, quanto piuttosto che la legge sia sufficientemente chiara nell'indicare le circostanze e le condizioni in cui le autorità pubbliche hanno il potere di ricorrere a misure di sorveglianza che invadono la vita privata dei cittadini

- [ ] Con particolare riferimento alla sorveglianza segreta, dal momento che essa per definizione non è aperta al controllo dei cittadini, la Corte ha affermato che sarebbe in contrasto con uno stato democratico accordare all'esecutivo o al potere giudiziario un potere illimitato

- [ ] Nella causa Libery v. UK (2008) la Corte ha giudicato l'Interception of Communications Act del 1985 (poi sostituito dal RIPA) non conforme all'art.8 CEDU

- [ ] Nella causa Kennedy v. UK (2010) la Corte ha giudicato il RIPA, con riferimento alle comunicazioni interne, conforme all'art.8 CEDU

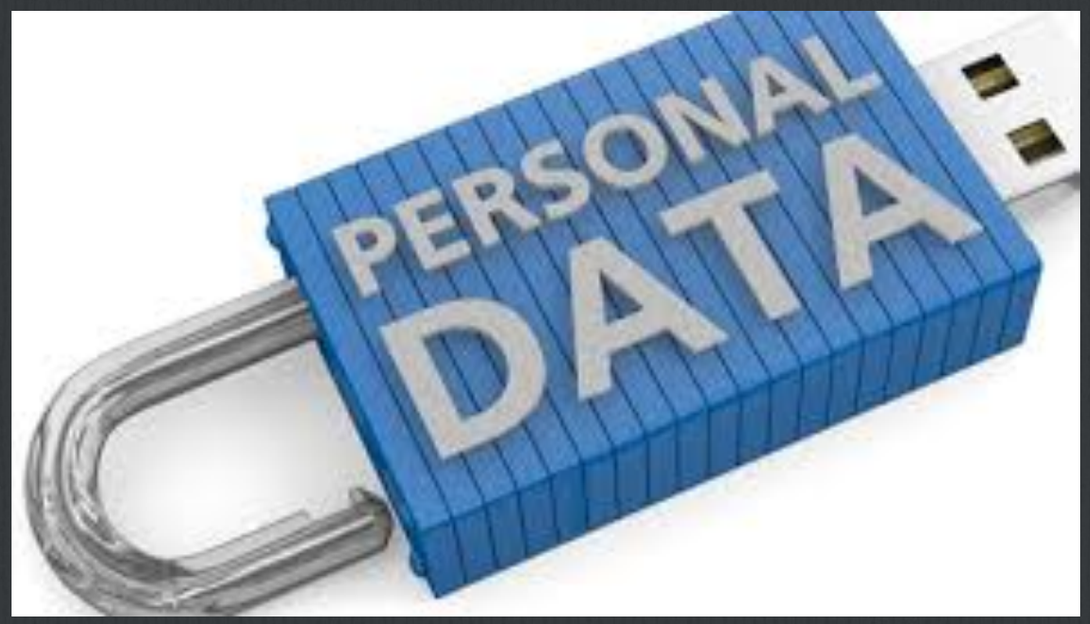
- Nella causa Weber v. Germany (2006) la Corte ha stabilito che la sorveglianza segreta è legittima solo se una legge stabilisce le condizioni per evitare abusi di potere; la legge dovrebbe contenere:

- un elenco degli illeciti che possono giustificare le intercettazioni
- un elenco dei soggetti intercettabili
- un limite nella durata delle intercettazioni
- le procedure per analizzare e conservare i dati ottenuti
- le precauzioni da adottare nei confronti di soggetti terzi
- le ipotesi di cancellazione e distruzione delle comunicazioni

Nel ricorso avanti l'Investigatory Powers Tribunal, Privacy International ha sostenuto che, nel caso PRISM, non vi è alcuna legge di copertura in quanto il RIPA è stato bypassato: non esiste quindi nessuna norma di diritto interno su cui parametrare i requisiti di cui all'art.8 CEDU

Nel ricorso avanti l'Investigatory Powers Tribunal, Privacy International ha sostenuto che, nel caso TEMPORA, c'è una violazione dell'art.8 CEDU in quanto il RIPA non autorizza la sorveglianza di massa: l'operazione di intelligence è sproporzionata ed ingiustificata

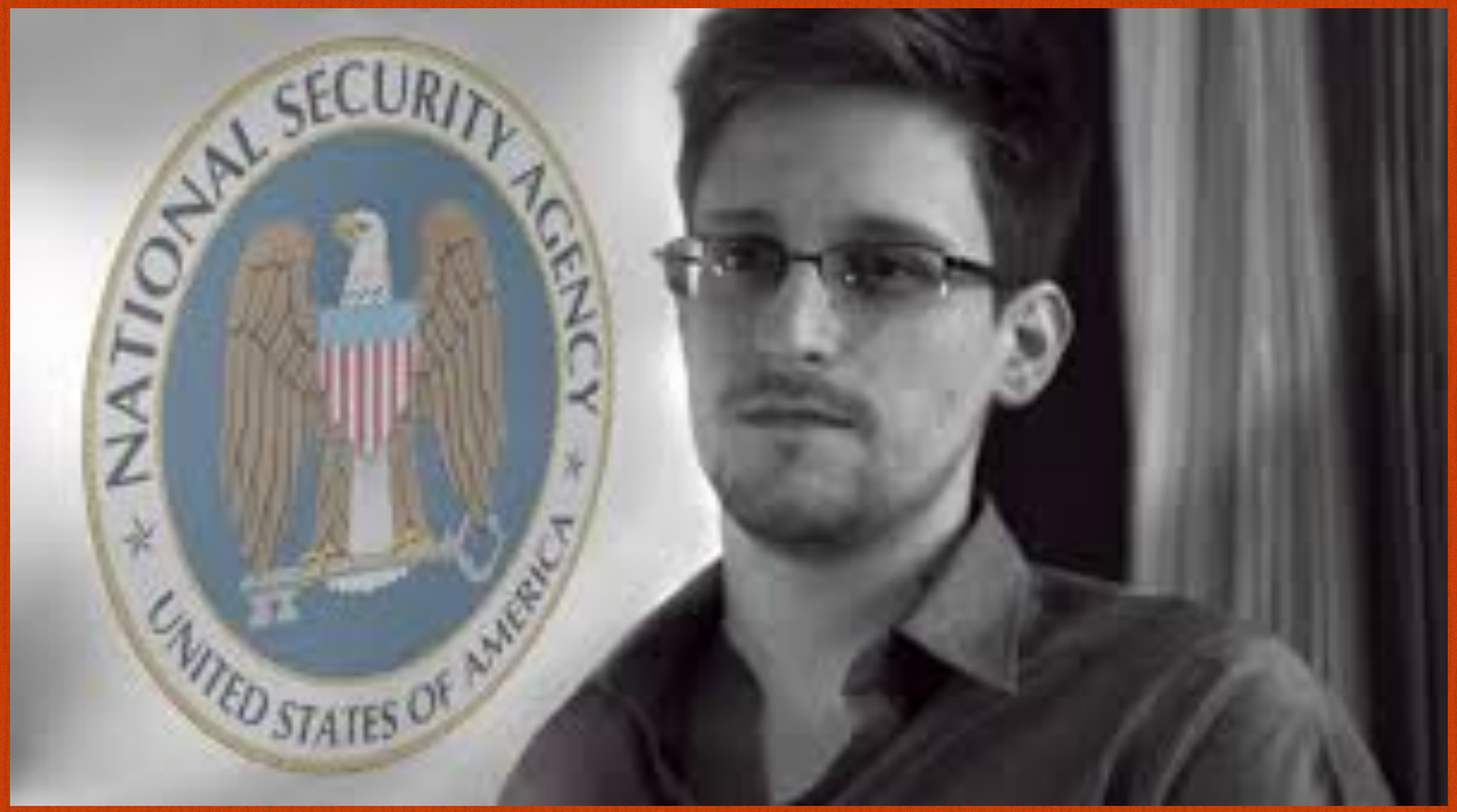
...e la data protection?



Possiamo dire che il trattamento effettuato dagli inglesi sui dati raccolti legittimamente dagli americani relativi ai sudditi di Sua Maestà è illecito?

...se è un trattamento illecito, quale tutela?

- ☐ Le direttive privacy e e-privacy non si applicano ai trattamenti effettuati dagli Stati per ragioni di sicurezza
- ☐ La prossima direttiva sul trattamento dei dati giudiziari non si applica perché riguarderà trattamenti effettuati nell'ambito di un procedimento penale
- ☐ L'art.8 della Carta dei diritti fondamentali UE potrebbe essere azionato?



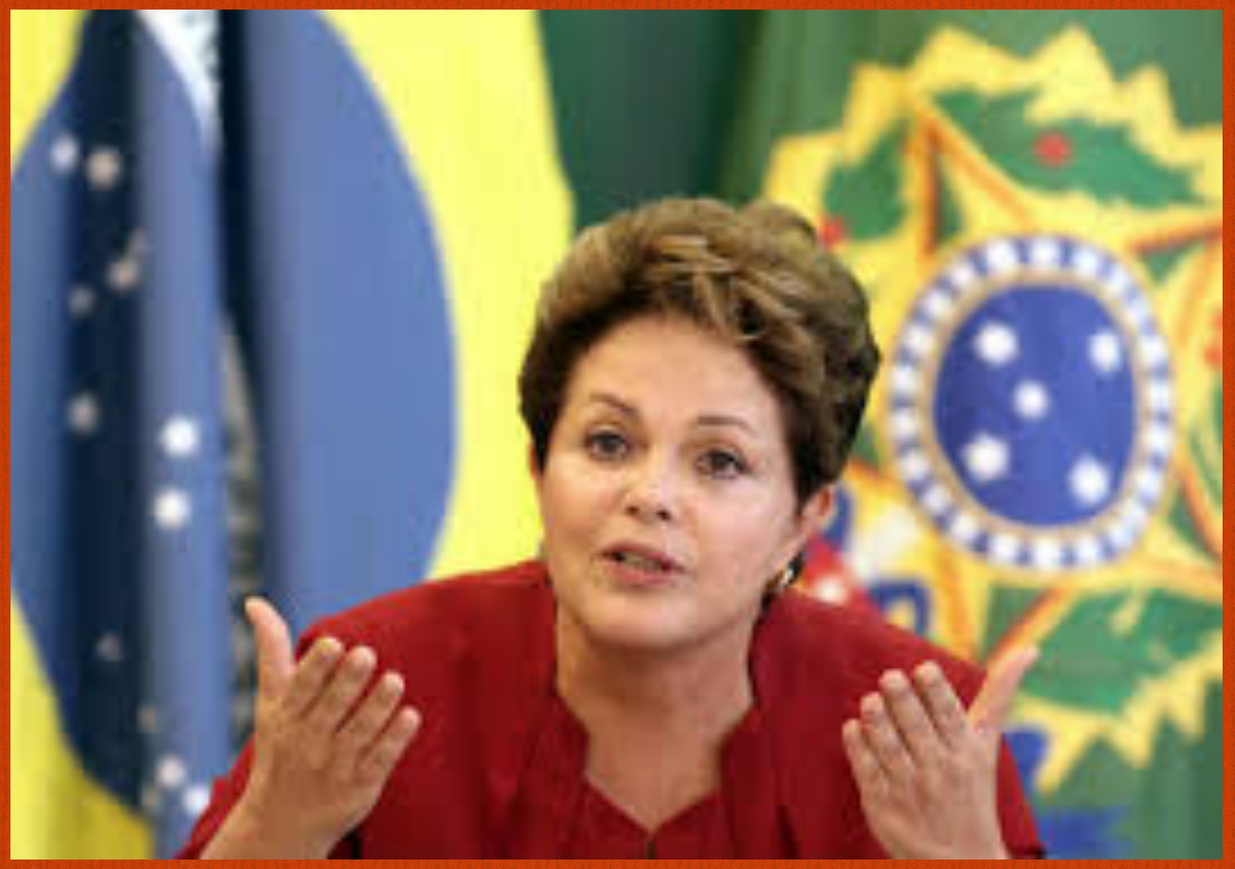
"Such programs are not just a threat to privacy, but to free expression and open societies"

Edward Snowden, Ein Manifest für die Wahrheit, Der Spiegel 45/2013

La data protection, è un diritto fondamentale che va riconosciuto e tutelato in maniera forte perché veicola le altre libertà fondamentali e con esse lo stato di diritto

"In the absence of the right to privacy, there can be no true freedom of expression and opinion, and therefore no effective democracy"

Dilma Rousseff



Grazie!

Monica A. Senor
www.penalistiassociati.it
senor@penalistiassociati.it
@masenor