

# Il Datagate e l'ipocrisia delle istituzioni

*Intercettare tutto e tutti  
è una pratica diffusa  
ovunque. Gridare  
allo scandalo è inutile.*

**I**l Datagate, lo scandalo suscitato da una gola profonda che ha rivelato al mondo l'esistenza e l'estensione del progetto statunitense di intercettazione globale chiamato Prism, ha provocato un gran rumore sui mezzi di informazione e qualche imbarazzo a livello diplomatico ma non è niente di nuovo. Nessuna legge, infatti, vieta a uno Stato di spiare un altro. E ciascuno Stato, quando sono in gioco interessi nazionali, al proprio interno fa quello che vuole anche "oltre" la legge. Ogni volta che filtra la notizia di questo o quel caso, dopo qualche tempo di vibrante protesta e giustificazioni istituzionali più o meno risibili, le cose tornano come prima. Gli stati intercettano e schedano, politici e garanti tranquillizzano i cittadini sull'esistenza di "ferree leggi" a loro tutela, e il gioco ricomincia. Ora, che gli Usa, quando si tratta della loro sicurezza, non guardino in faccia nessuno è un fatto notorio. Limitandoci alla tecnologia e agli ultimi trent'anni, basta ricordare il caso del Clipper Chip, in auge fra il 1993 e il 1996, un criptochip sviluppato dalla National Security Agency che sulla carta avrebbe dovuto garantire la sicurezza delle comunicazioni telefoniche, ma che in realtà conteneva una backdoor che consentiva a servizi segreti e assimilati di ascoltare le telefonate.

**Sempre dalla Nsa**, già prima del 2000, arrivò Echelon, un network di intercettazioni che coinvolgeva Usa, Inghilterra, Australia, Canada e Nuova Zelanda e che fu oggetto dell'inevitabile scandalo giornalistico, altrettanto inevitabilmente finito nel nulla, analogamente a quanto accadrà per Prism nella sua versione americana e in quella italiana.

Sì, perché anche l'Italia ha il suo Prism, meno tecnologico di quello

d'oltreoceano perché fatto di leggi e non di hardware e software, ma che consente comunque ai servizi segreti di accedere senza alcun controllo da parte della magistratura a qualsiasi dato in possesso di operatori telefonici, Isp e soggetti che gestiscono infrastrutture critiche (reti energetiche, ferroviarie, aeree, stradali e aeree).

Si tratta del Decreto del Presidente del Consiglio dei ministri (DPCM) 24 gennaio 2013 "Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale". L'articolo 11 di questo decreto stabilisce che «Gli operatori privati che forniscono reti pubbliche di comunicazione o servizi di comunicazione elettronica accessibili al pubblico, quelli che gestiscono infrastrutture critiche di rilievo nazionale ed europeo, il cui funzionamento è condizionato dall'operatività di sistemi informatici e telematici forniscono informazioni agli organismi di informazione per la sicurezza e consentono ad essi l'accesso alle banche dati d'interesse ai fini della sicurezza cibernetica di rispettiva pertinenza». Una volta tanto, il legalese è chiaro: i servizi segreti possono accedere direttamente a tutti – tutti – i database pubblici e privati esistenti in Italia, senza alcun effettivo controllo.

Questa norma è complementare a quelle che, a partire dal 2001 e in varie versioni fino al 2012, con la scusa di combattere il terrorismo, hanno legalizzato le intercettazioni preventive da parte dei servizi segreti in assenza di una indagine penale in corso.

Come se non bastasse, anche sul fronte delle indagini di polizia giudiziaria tocca registrare la crescente pressione che gli investigatori stanno esercitando su operatori telefonici e internet provider per ottenere dati e informazioni senza troppi fardelli

burocratici (leggi, applicazione delle garanzie previste dal codice di procedura penale). E così capita di vedere richieste di accesso a dati di traffico inviate via semplice mail, blocchi su DNS spacciati come "sequestri" e processi per accesso abusivo senza nemmeno il corpo del reato, cioè il server "bucato". Per non parlare di quello che accadrà quando qualche pubblico ministero si accorgerà che negli ospedali e nei laboratori di analisi esistono, in modo più o meno strutturato, delle biobanche di tessuti con annessa identità personale del paziente. Invece di attendere l'arrivo del data-base nazionale del Dna (ancora lontano da venire, e comunque a contenuti limitati agli autori di un certo tipo di reati), qui ed ora è già disponibile un'enorme mole di dati genetici che consentirebbero di identificare potenziali criminali che, almeno una volta, si sono fatti curare. Altro che profilazione delle abitudini di consumo, preoccupazioni per la pervasività di Google o di Facebook... La realtà è che la legge è uno strumento inutile e inefficace per proteggere i cittadini da un presente invasivo che, però, i cittadini stessi hanno contribuito a creare non preoccupandosi minimamente di quello che facevano della loro connessione a Internet.

**Allora**, è evidente che il problema di una vita a privacy zero non è tecnologico, ma culturale. Le uniche tutele efficaci sono, da un lato, far circolare quante meno informazioni possibili su di noi. Un dato che non c'è non può essere intercettato.

Dall'altro lato, però, invece di pensare ad usare le tecnologie solo per "difenderci" dalle invasioni della sfera personale, dovremmo pensare di utilizzarle per controllare i controllori. Anche se il risultato potrebbe non piacerci. •