La difficile convivenza tra intelligence e privacy nell'era del cybercrime. Ruolo e natura degli hackers al servizio degli Stati

di **Sergio Falcone** e **Mario Scaramella**

1. INTRODUZIONE

Il 566 Squadrone Intelligence presso lo Space Command della US Air Force a Buckley, Aurora, Colorado ascolta le comunicazioni elettroniche per conto della National Security Agency. Lo fa anche l'omologo Comando a Menwith Hill, Harrogate Yorkshire, in Inghilterra o il Comando congiunto a Pine Gap nel cuore del continente australiano, tutti ascoltano le comunicazioni elettroniche. I russi fanno lo stesso, sia dal suolo patrio che da basi sparse nel mondo come a Cuba, i Cinesi idem, anche da un centro in Argentina. Il sistema di ascolti Echelon[1] è probabilmente il più formidabile strumento di difesa e sicurezza occidentale condiviso dai paesi anglofoni. Anche in Italia opera dalla base della intelligence a Cerveteri e dalla nave ammiraglia della VI Flotta di stanza a Gaeta, la Mount Withney che ospita personale della NSA[2]. Tutti questi comandi spiano con grande impiego di mezzi, satelliti, misure elettroniche ed ascoltano potenzialmente tutto quanto sia sussurrato per telefono, per cable, per radio o captato da microfoni ambientali, inoltre osservano immagini, decrittano segnali, il tutto in ossequio a prassi internazionali, regole interne, regionali ed a regolamenti molto scrupolosi. A ciascuno è vietato spiare i propri concittadini ed altissimo è il livello di counter intelligence interno, le spie sono spiatissime perché non facciano danni. La NATO[3] ha sia

1 Echelon: sistema mondiale d'intercettazione delle comunicazioni private e pubbliche, per conto dei cinque stati firmatari dell'accordo UKUSA di sicurezza (Australia, Canada, Nuova Zelanda, Regno Unito e gli Stati Uniti).

2 NSA, National Security Agency, l'agenzia per la sicurezza nazionale degli USA.

3 NATO, North Atlantic Treaty Organisation, l'organizzazione del trattato dell'Atlantico del nord.

un nucleo di counter intelligence elettronica, centralizzato, sia i propri strumenti di ascolto, anche in Italia al Lago Patria sede del Comando Alleato per il Sud Europa dove vi è un centro SIGINT[4], Signal Intelligence. Nell'ambito del II Reparto Informazioni e Sicurezza alle dipendenze dello Stato Maggiore della Difesa italiana opera una rete di centri di ascolto e di difesa elettronica simili a quanto descritto per gli americani e le altre potenze, stessa funzione, stesse regole di ingaggio: specialisti militari e a volte civili molto competenti, molto controllati, con limitazioni strettissime, proporzionate al potere affidato alle loro mani.
Cosa accade nell'ambito della Pubblica Amministrazione, dei civili? Solo l'Autoritá Giudiziaria ha di fatto il potere di ascoltare le comunicazioni elettroniche (anche le c.d. preventive dei servizi segreti vanno autorizzate dalla Procura Generale di Roma) che, come fanno anche le aziende ed i privati, generalmente si avvale di consulenti informatici, esperti hackers.
In questo quadro tanto articolato quanto complesso si staglia una figura controversa qual è quella dell'hacker, abile a bypassare il confine del lecito senza però essere additato necessariamente come criminale, nonostante si appropri illegalmente di dati altrui e sia dotato, per sua stessa natura, di un'elevata pericolosità sociale. Negli attuali contesti professionali, culturali, e persino istituzionali, l'hacker incarna l'ideale di un Arsenio Lupin del 3° millennio la cui attitudine al crimine, sebbene cyber, è innestata di fatto nel sistema, il cui dark side assume una connotazione di romantica missione positiva o di efficiente cinismo cui il cittadino guarda con rispetto ed accettazione piena. Riunioni di hackers, convegni di crackers, associazioni di pirati informatici cui soggetti provenienti da molteplici contesti sempre più spesso si rivolgono, come se il ladro di dati fosse un perito, capace di esperire alte consulenze. E la missione politica, intellettuale, morale dell'hacker? Imprescindibile nella community il ruolo chiave di chi accede ai santuari, data-whare-house delle più autorevoli istituzioni per lasciar poi trapelare distillate informazioni il cui uso, in quanto manipolabile, apre la strada ad inquietanti scenari sui cui esiti evidentemente la società post-moderna non è in grado di riflettere con la dovuta consapevolezza e maturità. All'hacker è finanche concesso di violare gli inviolabili centri di ascolto militari perché possa poi pubblicare tutto su "Wiki" piattaforme, impunitá e gloria in quei casi, perché i pirati mascherati violano le istituzioni in nome del popolo sovrano del web, nell'era dove quel che arriva da Wikileaks[5] su Wikipedia[6] è verita, Verbo.
E sì, perché l'era della enciclopedia Treccani è passata. A pronunciarsi autorevolmente su questa o quella voce non è il best-in-class fra i massimi specialisti di ciascuna materia, magari accademico maturo con decenni di immacolato background e verificata credibilitá, ma l'interprete originale ed assoluto del vero è ormai l'incompetente

4 SIGINT, SIGnlas INTelligence, spionaggio di centrali elettromagnetici.

5 WIKILEAKS, organizzazione internazionale senza scopo di lucro che riceve, sotto forma di anonimato, documenti di carattere governativo o aziendale.

6 WIKIPEDIA, enciclopedia virtuale presente sul web, creata ed edita da volontari di tutto il mondo sotto l'egida di Wikipedia Foundation.

e smanettone, o l'hacker che ruba il "segreto" e lo divulga con modalitá e soprattutto finalità che rimandano all'utilizzo di strumentalizzazioni che allontanano inesorabilmente l'ignaro utente dalla verità.
Anonymous[7], network di spie informatiche, operativo anche fuori dal web con tanto di incursioni fisiche contro obiettivi strategici e riunioni cospirative dei suoi membri degne di una moderna banda Baader-Meinhof[8], sigle varie ed improbabili attive nel deep web, la parte profonda di internet, tanti self styled cyber experts, fanno la parte degli squali e contemporaneamente dei bagnini nelle acque scure del cyber oceano.
Questa è la cornice di un fenomeno, di una minaccia alla sicurezza democratica che questo articolo vuole approcciare: in un mondo virtuale dove l'operatore più smart è come minimo un borderliner, le istituzioni pubbliche e private hanno adottato il medesimo assetto verso la moderna infrastruttura, lontane dagli standard militari, affidandosi ad operatori che travalicano in alcuni casi il confine del lecito fino a delineare ritratti a tinte fosche di una realtà inquietante tanto è pericolosa. Ci troviamo di fronte ad una "cybercrime di Stato", quindi, affidata a moderni gangsters, dimostratisi più produttivi di quei soldati in divisa dei Comandi spaziali intenti ad ascoltare via satellite i segreti dai navigli e distaccamenti nemici? È impresa a dir poco ardua formulare una risposta esaudiente a questo come a tanti, innumerevoli interrogativi che si stagliano sull'orizzonte di questa epoca storica così fluida e inafferrabile, ma non ci è dato modo di procrastinare oltre. L'era della nuova e ben più radicale rivoluzione digitale, quella di cui l'IA[9] sarà l'artefice indiscussa, bussa alle nostre porte. È vietato indugiare.
È bastato l'approccio della Common Law britannica, che non conosce il limite di "*societas delinquere non potest*" e che in effetti è brocardo romano- napoleonico, alle azioni del Cremlino sul proprio suolo isolano (omicidio e tentato omicidio di dissidenti dei servizi segreti commesso in Inghilterra da incaricati dell'apparato Statale con modalità iperboliche, peraltro) per qualificare quei fatti come delitti commessi dallo Stato della Federazione Russa. Non parliamo di una delle tante aggettivazioni da tribuna politica o da letteratura divulgativa, citiamo sentenze e decisioni della Alta Corte britannica emesse in nome di Sua Maestà (da noi si direbbe in nome del popolo italiano).
Ma se lo Stato compie delitti, e la Federazione Russa non è certo l'unico paese che metta in essere attivitá coincidenti con fattispecie delittuose vere e proprie (si pensi agli altri paesi che per esigenze di sicurezza nazionale arrivano ad eliminare individui ostili sul territorio di altri membri della comunità internazionale, attovità rivendicata da USA ed Israele per esempio) e se è vero che alcuni giurisdizioni di fatto confliggano con le giurisdizioni altrui tanto da creare inevitabili rompicapo giuridici e scontri politici fra Paesi (ad esempio la giurisdizione extraterritoriale nei dieci casi di scuola previsti dall'ordinamento americano, non si limita alla possibilità di celebrare in patria

7 ANONYMOUS, fenomeno internet di attivismo in cui confluiscono soggetti singoli o raggruppati in comunità che agiscono con modalità anonima perseguendo un obiettivo comune concordato.

8 Gruppo anarchico-terroristico di estrema sinistra altrimenti noto come RAF, Rote Armee Fraktioon, operante dalla fine degli anni '60 in Germania.

9 IA, Intelligenza Artificiale, abilità di un computer di svolgere funzioni e ragionamenti tipici della mente umana in modo autonomo.

processi per vittime americane contro rei contumaci rifugiatisi all'estero, ma autorizza l'autoritá ad andarsi a prendere il reo all'estero, cozzando con la sovranità e giurisdizione del paese terzo..) cosa accade oggi nel cyber world?
La teoria e la tecnica dell'hackeraggio sono la nuova bibbia per individui, società e Stati. Il metodo criminale dei ladri di dati è assunto a modello per le massime istituzioni e, si badi bene, non solo per le modalità di accesso alle informazioni altrui, rubate crackando i sistemi informatici e le reti, ma soprattutto nella gestione della filiera dove utilizzo, selezione, distillazione, manipolazione, falsificazione e diffusione dei dati sono minacce alla sicurezza ben maggiori del furto *in re ipsa*. Crimini elettronici di Stato compiuti attraverso delinquenti comuni, simili a quegli assassini di Stato che la giustizia inglese già ha censurato.
Ma è una storia vecchia come il mondo dell'elettronica, qualcuno potrebbe dire, con la prima comunicazione radio sono nati gli intercettatori di comunicazioni, con i codici sono nati i decifratori e con internet gli hackers, i governi si avvalgono da sempre di "illegali" per monitorare e difendere i propri interessi nelle comunicazioni… ma non è così. Il punto su cui la nostra ricerca vuole evidenziare un livello di minaccia alla sicurezza democratica dei nostri ordinamenti cui non si era mai giunti è esattamente questo: l'attuale prassi nell'utilizzo del mondo virtuale da parte di alcuni Stati nazionali è tecnicamente e giuridicamente criminale, affidata a criminali e del tutto fuori controllo per gli stessi Stati committenti. La minaccia di divulgazione di dati, ancor peggio laddove fosse manipolata, su piattaforme in grado di raggiungere con un click un pubblico vasto quanto mai prima di ora, pone feroci e urgenti interrogativi a cui le società sono eticamente, prima ancora che giuridicamente, chiamate a rispondere. Ciò non era mai avvenuto nella prima era delle comunicazioni e nel novello cybermondo.
Sul piano civile del tutto innocue le attività dei militari, *tanquam non esset*, visto che i dati acquisiti non possono essere trasmessi alle autorità civili. I data base antiterrorismo americani come il TIDE[10], compilati con i dati di intelligence elettronica che schedano i sospetti, non possono essere passati all'FBI[11] ma restano roba per spie; in Gran Bretagna le intercettazioni elettroniche operate dal GCHQ[12] non sono mai utilizzabili per processi, anzi nessuna intercettazione lo è. Il giudice nazionale che autorizzava intercettazioni di comunicazioni effettuate dall' estero, interferendo nella banda elettromagnetica ma all' interno del proprio territorio e giurisdizione, appariva già di per sé invadente. È il caso di tante inchieste internazionali che hanno monitorato trafficanti stranieri operanti in Italia, ad esempio; ma quando poi quel giudice ha cominciato ad intercettare telefonini stranieri gestiti da operatore estero ed utilizzati da soggetti situati fuori dalla giurisdizione, come sono state qualificate quelle misure tecniche se non

10 TIDE, Terrorist Identities Datamart Environment, database antiterrorismo della intelligence USA. Riunisce i database istituzionali che censiscono i nominative delle persone a rischio, gestito dal National Counter Terrorism Center N.C.T.C. . Il TIDE censisce oltre 300.00 nominativi di potenziali sospetti e 200.000 schede specifiche su terroristi ed è collegabile ad altri database e security lists, al Sistema visti del Dipartimento di Stato (USA), ai database sui passaporti e ai sistemi di controllo frontaliero.

11 FBI, Federal Bureau of Investigation, ente investigativo di polizia federale degli USA.

12 GCHQ, Government Communication HeadQuarter, intelligence elettronica centrale del Regno Unito.

spionaggio di Stato? Legali sì, ma solo per l'autorità inquirente mentre oggettivamente violative di leggi e trattati internazionali oltre che delle altrui legislazioni e sovranità. Ma cosa accade quando addirittura quella forzatura viene compiuta da una autorità non con i mezzi e gli uomini dell'apparato statale (quali poliziotti, finanzieri, carabinieri, ufficiali della polizia giudiziaria all' interno di postazioni di ascolto, situate nelle procure o nei comandi) ma in outsourcing con gli hackers, consulenti tecnici, expert witnesses?
Il passato delle operazioni illegali di Stato ci dice che mai gli ascolti sono stati affidati e commissionati a privati.
Gli autori di questa ricerca hanno effettuato accesso presso l'Università di Cambridge, Churchill College, Churchill Archive Center; su autorizzazione del competente archivista, hanno avuto accesso ai voluminosi carteggi depositati dal Governo britannico (Manuscript extracts from KGB first chief directorate files Mitn 2/2 Envelope K2 Europe Items 1/428 e ss.) e relativi alla collezione di atti ed appunti redatti da un ex archivista del servizio di sicurezza dello Stato ai tempi della Unione Sovietica. Trattasi del cd. Dossier Impedian trasmesso nel 1995 dalla intelligence britannica a molti servizi collegati fra cui l'italiano SISMI[13] e da cui furono sviluppate inchieste giudiziarie dalla Procura di Roma e parlamentari fra cui una commissione bicamerale di inchiesta nella XIV Legislatura e che nella sua versione integrale era andato smarrito o "lost in translation" (vd. appendice). Ebbene è stato possibile individuare carteggi inediti e mai rivelati che descrivono compiutamente le modalità e tecniche dell'ascolto illegale delle comunicazioni italiane da parte della esplorazione sovietica che gestiva un sistema di antenne speciali per la captazione di segnali elettronici ed effettuava ascolti sul Palazzo di Giustizia di Roma in Piazzale Clodio, aveva antenne disseminate in tutta Italia e una base nella Ambasciata russa di villa Abamelik in Roma. L'ascolto non era poco rilevante per la politica, economia e sicurezza italiana e dei paesi alleati, se si considera che l'intero cable cifrato di Acilia era doppiato e praticamente ogni comunicazione monitorata. L'operazione Start, che ha riguardato gli anni '80 ed è stata poi riorganizzata in successive operazioni Start 2 etc.. ha costituito un successo indiscutibile per quello Stato a danno del nostro paese e degli alleati NATO indirettamente spiati, ma per quanto ci riguarda ai fini della presente ricerca ha dimostrato un approccio molto professionale, sicuro, segreto, istituzionale della intelligence elettronica di quei tempi, similmente a quanto gli USA realizzavano costruendo appositi sottomarini (del costo di mezzo miliardo di dollari ciascuno!) per entrare in acque sovietiche ed intercettare i cable fra basi isolane e a terraferma.
Ebbene i militari con i loro mezzi e personale, segretamente e professionalmente si tenevano reciprocamente informati su quanto il nemico dicesse, il modello era esteso alla intelligence politica e giudiziaria, utilizzavano apparati e personale qualificato, dipendente (i russi impiegavano al massimo le consorti dei funzionari del KGB[14] per

13 SISMI, Servizio Informazioni e Sicurezza MIlitare, servizio segreto italiano attivo dal 1977 al 2007.

14 KGB, Komitet Gosudarstvennoj Bezopasnosti, principale agenzia di sicurezza, servizio segreto e polizia segreta dell'Unione Sovietica.

gli ascolti, ed ingegneri militari, per contenere la diffusione delle informazioni, nessun esterno o civile era coinvolto) e di tutte le informazioni rubate ben poche sono uscite dai cassetti blindati e dalle casseforti dei servizi. L'utilizzo di queste informazioni era limitatissimo, altri direttorati, ad esempio il V per le misure attive del KGB si occupavano in maniera molto competente di divulgare informazioni vere ed altre fasulle sul proprio paese e sui nemici, manipolando certamente e tecnicamente selezionando, distillando, analizzando ogni dato al fine di comunicare con la tecnica della propaganda le proprie idee ed esercitando proverbiale influenza sulle masse. Ad est ed a ovest la guerra fredda è stata combattuta anche e soprattutto con una potente propaganda che si basava su informazioni rubate al nemico, questo lo schema che per noi deve essere un riferimento nell'era della seconda guerra fredda con i paesi dell'Est, Federazione Russa ma anche Cina, Corea del Nord, Iran.
Questa ricerca parte quindi dalla constatazione che l'intelligence elettronica durante i tempi della contrapposizione dei due blocchi NATO/Patto di Varsavia, era esercitata con metodo sostanzialmente esplorativo da servizi segreti ma nell'ambito delle prassi potremmo dire istituzionali di chi deve esercitare la propria sovranitá, anche ascoltando e monitorando tutto quanto accessibile. L'attuale contrapposizione fra paesi oggi diversamente allineati (basti pensare che Cina e Russia un tempo irriducibili nemici sono oggi uniti dal Patto di Shanghai e costituiscono un unicum in termini di difesa e cyber security, così come la Corea del Nord e l'Iran che devono alla Russia tutto il proprio know-how elettronico e tecnologico in generale) si realizza in potenti operazioni di ascolto e in propaganda, come ai vecchi tempi, ma con strumenti e dinamiche totalmente differenti.
Siamo nell'era dei social, nell'epoca di Wikipedia, delle società di profilazione utenti come la famigerata Cambridge Analytica[15], nel tempo in cui società private facenti capo ad hackers e aziende private senza scrupoli svolgono quella funzione cospirativa di furto dei dati personali, elaborazione e propalazione di contenuti al grande pubblico dei social con tecniche di psicologia sociale talmente efficaci quando massicciamente impiegate poi dal committente statale, da modificare l'esito delle elezioni politiche di grandi paesi (si pensi al data gate durante le presidenziali USA), referendum (si pensi alla Brexit) oltre che ovviamente capaci di fare da filtro nazionale alle idee di liberta' ed alle veritá provenienti da altrove.
Siamo nell'era in cui gli stessi Stati sovrani hanno affidato a privati dal profilo di impiego spiccatamente criminale e sovversivo la propria "sicurezza" elettronica, nell'età dell'elettronica, peraltro.
Attualmente in Italia le intercettazioni telematiche, consentite solo nei procedimenti per reati di mafia e terrorismo fino al recente dettato della legge anticorruzione n. 3/2019 pubblicata su G.U. n. 13 del 16/1/2019 cd. "spazzacorrotti" che estende a tutte le ipotesi di reati contro la P.A. (inclusi i nuovi reati di traffico influenze illecite, art. 346 tris C.P., ed ai neoformulati 318 C.P. corruzione per l'esercizio della funzione, 646 C.P.

15 CAMBRIDGE ANALYTICA, è stata una società di consulenza britannica celebre per lo scandalo emerso nel 2018 connesso alla gestione dei dati utilizzati per influenzare le campagne elettorali.

appropriazione indebita, al 2635 bis C.P. corruzione fra privati ed alla corruzione fra privati etc.) ed in particolare ai reati compiuti da italiani o stranieri all' estero (modifica degli artt. 9 e 10 del Codice Penale) con stravolgimento dei principi generali del diritto penale, sono possibili attraverso l'installazione di appositi "Trojan"[16] nei dispositivi degli indagati. Quali le competenze all' interno delle forze di polizia? La Guardia di Finanza disponeva di apposito Comando GAT[17] presso il Comando Generale per le attività tecniche informatiche che però è stato sciolto. Informatici nel Servizio Operazioni del Comando Generale e nei nuclei di Polizia Tributaria o altri comandi appaiono inseriti in organico in maniera discontinua e fanno fronte soprattutto alle esigenze organizzative interne del Corpo e non hanno un profilo di impiego operativo, i Compartimenti di Polizia Postale e delle Telecomunicazioni della Polizia di Stato non dispongono di specifiche attrezzature o know-how, limitato al Centro Nazionale di Polizia delle Telecomunicazioni che però si avvale generalmente di consulenti esterni, i Comandi territoriali dei Carabinieri parimenti non dispongono di operativi per le cyber indagini e le competenze sono limitate ai RIS e a pochissime articolazioni specialistiche. Gli esperti per l'installazione e gestione di Trojan, cioè virus, sono reclutati dalle Procure fra gli hackers….. un po' come affidare la sicurezza domestica e le chiavi di casa ai ladri pregiudicati del quartiere.
Esistono ovviamente competenze a livello nazionale ma i servizi per la sicurezza e le informazioni, l'AISE[18] per l'estero e l'AISI[19] interna, che formalmente possono svolgere intercettazioni preventive solo con l'autorizzazione preventiva della Procura Generale di Roma (che ha predisposto una sala presso la propria sede) per numero di richieste alla A.G.[20] dimostrano di avere un vissuto quasi completamente extra giudiziario ed un profilo di impiego del tutto indipendente. Così come indipendenti sono i grandi centri di ascolto quali Cerveteri, gestiti in ambito Echelon o NATO peraltro, i comandi dipendenti dal Ministero della Difesa e sopratutto dal II Reparto, che svolgono funzioni strettamente legate alla difesa militare ed il tentativo di coordinamento affidato al DIS, Dipartimento Informazioni e Sicurezza della Presidenza del Consiglio, è ripetutamente naufragato fra le alternative visioni dei Governi succedutisi e le ambizioni personali dei titolari nazionali della nostrana Cybersecurity, che dovrebbe spettare alla Difesa ma è sempre soffocata dai burocrati della PCM[21]. L' Industria nazionale parimenti non ha brillato per iniziativa concentrandosi a livello di Finmeccanica - Leonardo SPA su standard tecnici completamente ispirati, importati da paesi terzi quali Israele e senza assemblare, nel collage di software & hardware adottato le straordinarie competenze delle piccole imprese informatiche nazionali e delle importanti università, che pure

16 TROJAN, tipologia di malware che nasconde il suo funzionamento all'interno di un programma all'apparenza innocuo.

17 GAT, Gruppo Anticrimine Tecnologico della Guardia di Finanza in Italia.

18 AISE, Agenzia Informazioni e Sicurezza Esterna, servizio segreto italiano per l'estero.

19 AISI, Agenzia Informazioni e Sicurezza Interna, servizio segreto italiano delegato alla sicurezza interna.

20 A.G., Autorità Giudiziaria.

21 PCM. Presidenza del Consiglio dei Ministri italiano.

consentirebbero alti standards di impiego. Quando un potente gruppo di affaristi, i fratelli Occhionero, hanno hackerato decine e decine di istituzioni ed aziende italiane, incluse la Presidenza del Consiglio, la Difesa ed i Carabinieri[22], non solo nessuno se ne è accorto salvo il gruppo sicurezza dell' ENAV, Ente Nazionale Aviazione Civile, che ha sopperito con proprie competenze ed energie al gap istituzionale standard, ma quando la Procura di Roma si è attivata per verificare (l'un per cento nemmeno delle violazioni, accessi e dei danni realizzati dagli Occhionero tramite virus continuamente riaggiornati da un team -mai identificato- e tramite i computer già infettati), ebbene la difesa degli imputati ha potuto denunciare polizia postale e Pubblico Ministero per i propri reati informatici commessi tramite "consulenti" ed hackers nell' indagare i sospetti, tale il caos che regna, sopratutto a livello tecnico operativo.
Se quindi il fai da te nelle varie amministrazioni italiane è uno standard nella sicurezza difensiva da attacchi, lo è anche a livello di operazioni, legittimate, pianificate, autorizzate a livello di legislatore ed amministrazione centrale dello Stato ma realizzate qua e là con metodi improvvisati e con ricorso sistematico alla galassia dei cyber criminali.
Poiché la guerra informatica moderna, come pure la vecchia guerra fredda e le battaglie industriali, economiche e politiche non si limitano a soli accessi ed ascolti di informazioni ma sconfinano nella scientifica collezione, organizzazione, manipolazione, distillazione e propalazione delle stesse alle masse, così mediante gli accessi affidati ad hackers la propaganda è stata di fatto affidata dagli Stati a gruppi ben poco trasparenti.
Data Gate è la approfondita indagine che il Dipartimento di Giustizia federale americano ha condotto tramite un investigatore indipendente sulle elezioni presidenziali ed indirettamente sullo stesso Presidente degli Stati Uniti Donald Trump. La sola ipotesi accusatoria di per sé basterebbe a collocare tutta la problematica dell'accesso alle informazioni e della relativa manipolazione e propaganda nel più alto livello delle minacce alla sicurezza delle grandi democrazie. La sola teorizzazione che si possa influire sulla più alta espressione del popolo sovrano dovrebbe collocare la cyber security al top delle categorie ontologiche della *salus populi*. Ed in effetti così è.
Da quando si è compreso che il furto dei dati personali, dei dettagli intimi e privati di ciascuno degli utenti di questo e di quel social network, e che la somma di questi furti hanno consentito profilazioni accuratissime e conseguenti campagne di disinformazione, mirate ed adattate a ciascun individuo, e che il totale di queste mistificazioni ha prodotto condotte sociali alterate al livello del corpo elettorale di grandissimi paesi e solidissime democrazie, si sta correndo ai ripari.
Trump è stato eletto grazie alla pressione esercitata da Putin e dai suoi organi di controinformazione? non è esattamente così ma il fatto che 1) la Russia ci abbia provato, 2) l'infrastruttura si sia dimostrata fragile e 3) il risultato sia comunque una enorme pressione sull' establishment governativo centrale tale che la politica debba fare i conti con questa fenomenologia, è di per sé una emergenza epocale.
La Gran Bretagna non sarebbe nelle critiche condizioni di auto-implosione se non vi

22 Cfr. Ordinanza di custodia cautelare in carcere emessa dal Tribunale di Roma – sezione gip 37 del 5.1.2017 nell'ambito del procedimento n.ro 21245/16 RGNR.

fosse stata una forzatura sui numeri nel referendum pro Europa? Anche qui vi sono dinamiche molto più complesse della facile semplificazione, ma il fatto che vi sia un popolo sovrano soggetto alle influenze dei tecnici della psicologia sociale, che grazie ai social network ed alle loro falle riescono in ciò che la semplice propaganda dei media tradizionali non aveva mai potuto, ci spinge a riflettere.
Il fenomeno non è ovviamente limitato al Facebook di Zuckerberg o a quello di Usmanov, e non si è sperimentato solo nelle elezioni americane o nel referendum sulla brexit. Il ruolo di società come Cambridge Analytica, che hanno svolto il lavoro materiale di furto di dati e formulazione di profili con relative azioni di condizionamento delle masse, è molto più ampio e diffuso di quello che si può pensare. Il problema è anche culturale, paesi con elevata scolarizzazione come quelli scandinavi hanno, a livello di individui, una percezione del reale molto più accurata rispetto a paesi meno scolarizzati.
Volendo focalizzare l'analisi della problematica sui profili giuridici ed istituzionali e senza voler allargare alla cornice storica e culturale il fenomeno, è senza dubbio necessario approfondire quali strumenti offra concretamente il sistema per la difesa da questa incombente, epocale sciagura.
La dinamica che ci interessa arriva alla manipolazione della volontà delle masse, anche elettorali, come effetto, e parte dal furto di dati personali al fine di profilazione e quindi di condizionamento, come causa. Nel mezzo però c'è una enorme realtà, ovvero il mondo dell'informazione, che costituisce il teatro in cui la vittima di manipolazione arriva poi a soccombere causa i limiti, anche culturali, storici, economici e sociali, nell' accesso alla genuina informazione. Alcune considerazioni su questo mondo di mezzo che quindi costituisce la cassa di risonanza per la nota stonata che infine diventa rumore assordante.
Per definizione e per prassi consolidata gli Stati sia democratici che dittatoriali esercitano la propria sovranità anche e soprattutto attraverso l'intelligence, i servizi segreti. Gli Stati dunque acquisiscono e conservano le migliori informazioni politiche, militari, scientifiche, industriali, economiche con metodo spionistico e non rendono disponibili dette informazioni al pubblico. Questo crea una enorme distanza fra cittadino elettore e Governo che, seppure necessita di un vantaggio informativo sui paesi competitori, arriva a sacrificare il diritto fondamentale degli individui alla conoscenza, e soprattutto le dinamiche sociali che sono alla base del consenso popolare dei governi democratici.
Non solo politica internazionale ma anche scienza. La DARPA[23] del Pentagono per esempio sviluppa e custodisce segreti scientifici che il cittadino contribuente non può conoscere. Anche le modalità con cui l'esecutivo affronta sistematicamente alcune questioni non sono palesate, si pensi al ruolo nel Ministero degli Esteri italiano della c.d. Unità di Crisi che sembrerebbe gestire emergenze che in realtà sono sempre competenza di uffici della Presidenza del Consiglio, e che nella Unità diplomatica hanno solo una copertura. Questo il mondo delle istituzioni. In America come in Europa, in

23 DARPA, Defence Advanced Research Projects Agency, agenzia governativa del Dipartimento della Difesa degli Stati Uniti incaricata dello sviluppo di nuove tecnologie per uso militare.

Russia come in Cina o in Africa i governi sanno cose che ai cittadini non vengono comunicate, agiscono di conseguenza, salvo poi fare i conti con masse, anche elettorali laddove esiste cittadinanza attiva, inconsapevoli e impreparate. Gli Stati compensano la distanza informativa fra i governi e la cittadinanza attraverso i media, più o meno liberi, più o meno orientati e condizionati, attraverso la propaganda diretta, attraverso "misure attive" di cui erano e sono maestri soprattutto i regimi comunisti e post comunisti, attraverso il sostegno alla letteratura, alla enciclopedia, all'università, al cinema.
Società molto evolute, come quella inglese o francese, forti di gloriosa storia patria, amministrazione efficiente, cultura diffusa e sufficiente rapporto fiduciario fra cittadini ed amministratori, hanno retto per secoli affidando alla complessiva credibilità del governo ed alle verifiche democratiche o istituzionali di parlamenti, re, osservatori qualificati, l'equilibrio sociale fondamentale. Altre più fragili hanno spesso capitolato al momento della verifica di piazza dei governi di turno. Certo le società nell'era post napoleonica, e soprattutto successiva alle due guerre mondiali, sono società basate sul ruolo della legge, sui diritti, sull'accesso politico alle informazioni almeno fondamentali, anche se in realtà sono stati combattuti almeno 70 anni di guerre contro falsi bersagli (tipo USA vs Vietnam o URSS vs Afghanistan) laddove i veri giochi non erano palesati affatto, tanto da condizionare la politica interna di ciascun paese anche europeo in questioni essenziali come il terrorismo, il ruolo del comunismo, la mafia e molti affari religiosi. Veniamo dalla informazione a metà, siamo figli di una comunicazione di Stato che ci forniva solo parte delle notizie ma almeno ci offriva piattaforme certe, come le aule e commissioni parlamentari, le agenzie di notizie, i programmi scolastici, le enciclopedie e le università. Cosa è cambiato? Innanzitutto con il mondo virtuale i filtri fisici e materiali sono caduti, così che al giornale cartaceo che magari ometteva qualche notizia ma per il resto ci forniva dati qualificati e verificati, sono subentrati i social, i siti web autonomi e autoreferenziali, le piattaforme libere ma troppo libere tanto che nel mondo attuale ha la medesima visibilità potenziale uno scienziato premio nobel o un terrapiattista sconosciuto. Questo libero ed incontrollato accesso si è cristallizzato creando abnormi concentrazioni di potere e di visibilità proporzionali non alle referenze o credibilità istituzionali, ma alle mere capacità tecniche di basso grado di informatici e purtroppo di hackers. Non la singola libera informazione ha avuto successo, ma la sistematica collezione enciclopedica di dati non verificati e non verificabili. Ha trionfato la enciclopedizzazione dell'approssimativo se non del falso, la piattaforma su cui le moderne sfide alla sicurezza democratica si giocano. Siamo alla anarchia, alla platonica "democrazia".
Quali i risvolti ed i mezzi giuridici per difendersi nella moderna era in cui Wikipedia è il parametro di riferimento assoluto di verità? Ben pochi.
Qualora volessimo, ad esempio, contestare a Wikipedia una grande falsità, una bufala assoluta che impatta con una questione politica rilevante e che potrebbe avere effetti elettorali, ci scontreremmo contro difese inscalfibili. Il server della Wikipedia internazionale è in California, qualunque richiesta di dati può essere fatta solo per via giudiziaria quindi, per noi, con rogatoria internazionale. I tempi di conservazione dei dati, primo tra tutti degli identificativi IP degli utenti che compilano notizie sulla piatta-

forma, sono mantenuti per una durata inferiore al minimo possibile per una richiesta rogatoriale (giudice nazionale al proprio Ministro di Giustizia, da questi al Ministro Esteri da qui al Segretario di Stato, poi all'Attorney General quindi ad un giudice locale che finalmente chiederà da quale computer si è connesso l'amministratore Wikipediano sig. "Art-attack" che ha manipolato dati. Ebbene impossibile avere una risposta, parimenti se la Autorità Giudiziaria chiedendo alla Fondazione italiana di Wikipedia volesse adottare misure coercitive o di indagine invasiva non ne caverebbe un ragno dal buco perché i wikipediani italiani sono nascosti sotto l'ombrello della Wikipedia International. Ma se anche in tanti, inclusi gli Stati, stanno sbagliando, avvalendosi di ladri di dati per le istituzionali attivitá di monitoraggio e di fantomatiche società private per l'intelligence elettronica, ricordiamoci sempre che abbandonato lo Stato di diritto, c'è solo la barbarie, collettiva ed intima, individuale brutalità.
Sviluppo dei principi generali del diritto alla privacy, nell'ambito del diritto pubblico, a livello internazionale e comparato, nelle varie articolazioni dei nostri ordinamenti, questa la sfida epocale del giurista che auspichiamo salverà la comunità dal nuovo medioevo "informatico".

APPENDICE

Nel corso della ricerca di riscontri circa l'esistenza di parti non note del c.d. dossier Mitrokhin gli autori hanno acquisito notizia e poi copia di un file effettivamente compilato dall'ex Maggiore del KGB Vassilii Mitrokhin. Il file in questione, importante perché costituiva un esempio di testo NON ufficialmente pervenuto agli italiani e che viene riportato integralmente di seguito, è relativo a misure di captazione di comunicazioni radio e soprattutto dei cable per la Marina Militare della STET ad Acilia. La straordinarietà del documento non era solo relativa al fatto che esso costituisse prova di una selezione, da ignoti operata, sul materiale di provenienza Mitrokhin destinata all'Italia, ma anche nel merito indicava la rilevanza delle misure tecniche sovietiche.
- Pagina 114/punto 316 START postazione radio per l'ascolto clandestino di comunicazioni in Roma, tutto il personale consiste in 5 agenti più un ingegnere radio e quattro operatori, tutti gli operatori sono donne divenute mogli di agenti del KGB, ogni operatore ha lavorato al suo posto di ascolto per 20 ore alla settimana, la postazione funzionava 5 giorni alla settimana e lavorava circa sedici ore al giorno dalle sette del mattino alle 11 della sera ed in caso di necessità per 18 o 19 ore dalle 6,30 del mattino ed a volte funzionava il sabato ed in giorni festivi.
- Pagina 115 punto 317 Start START è una postazione di ascolto radio, di riacquisizione di informazioni in Roma che è stata istituita e organizzata con l'obiettivo di ricercare canali di informazioni e di raccogliere ed organizzare informazioni di valore relative a vaie operazioni del KGB. Nel 1976 ci sono state verifiche ed indagini sul funzionamento nel distretto di Roma ed una operazione per installare degli apparati che somigliassero ad antenne e le prime verifiche hanno riguardato gli edifici della Ambasciata sovietica a Roma, ovvero le postazioni costanti e permanenti localizzate negli edifici denominati

Abamelik, I vari tipi di antenne e sistemi sono stati verificati ed il risultato è che molti apparati e canali di comunicazioni riguardavano le direttrici fra Roma Pisa e Milano, cassette radio sono state utilizzate e 248 audiocassette con nastro magnetico sono state raccolte e sbobbinate nel 1976 il che ha costituito il punto di svolta con la ***creazione di ulteriori 18 nuove postazioni dedicate a cercare informazioni e 37 messaggi segreti sono stati raccolti da cinque cavi telefonici denominati YTK,*** *ben noti. Punto 318 la residenza romana del KGB ha deciso di effettuare sopralluoghi visivi e fotografici. Sopralluoghi nelle seguenti città italiane di* ***Acilia, Tenuta, Rocca Priora, per la zona sud di Roma, Palo per l'ovest di Roma e Fogliano, Morlupo, San Pancrazio per il Nord di Roma ed il sopralluogo ha verificato che fosse rispettata la qualità delle informazioni ri trasmesse delle antenne e dei radio nodi localizzati nel distretto di Roma****. Altri nomi di* ***luoghi dove erano installati punti di ascolto a Roma erano Inviolatella, Monte Mario, e piazzale Clodio****. Punto 319 postazioni radio di riascolto Start KGB residenza in Roma,* ***la presenza di centri operativi internazionali in questo paese, sopratutto l'importanza del centro di Acilia ha evidenziato l'importanza dell'Italia nel sistema delle comunicazioni globali e ricopre tutti i tipi di connessioni via cavo, connessioni via reti di antenne, via radiofrequenze e RRLS e di altro tipo nei distretti fra Milano e Roma attraverso la città di Firenze. I sistemi di controllo sono stati da noi collocati anche nei distretti fra Milano e Roma attraverso la città di Pisa, sei punti di raccolta informazioni sono localizzati e controllati nel distretto fra Roma e Napoli come in altre parti del sud Italia, nel distretto di Roma Inviolatella e del Monte Faete ci sono 7 posti di raccolta informazioni con antenne di differente diametro di portata di ascolto, localizzati e controllati*** *Pagina 128 paragrafo 351 l'Ambasciatore USSR in Roma di nome Maltseev ha acconsentito alla installazione di una nuova postazione denominata Start 2 nell'edificio localizzato nella Grande Villa Balshaia ed ha accordato che l' installazione sia posizionata sulla cima della stanza soggiorno, questo messaggio è stato ricevuto dalla residenza del KGB di Roma.*

Sergio Falcone: laurea in giurisprudenza alla Federico II di Napoli; avvocato patrocinante dinanzi alle giurisdizioni superiori. È specializziato nel diritto civile e commerciale ed in data protection. È certificato esperto in gestione aziendale. Dal 2007 ricopre la carica di Coordinatore della Commissione privacy e cyber security istituita dal Consiglio dell'Ordine degli Avvocati di Napoli. Negli ultimi venti anni ha pubblicato su diverse riviste giuridiche ed informatiche articoli e commenti in materia di privacy e sicurezza.
È consulente di grandi aziende e di Enti pubblici, svolgendo la funzione di Data Protection Officer.

Mario Scaramella: laurea in giurisprudenza alla Federico II di Napoli, studi post graduate in istituzioni di diritto pubblico e diritto internazionale, docente presso la Seconda Università degli Studi di Napoli Scuola di Alta Formazione Jean Monnet e presso la Federico II, Dipartimento di Studi Internazionalistici. Ha insegnato intelligence elettronica come Visiting Professor presso la Stanford University, Centro per la Coopera-

zione Internazionale nello Spazio Dipartimento Ingegneria Elettrica e come Research Fellow al Metropolitan Technology Center della Università della California, SJSU, presso la Base Aeronavale di Moffet Field NASA Ames. Svolge attivitá di consulente legale, "lawyer", a Londra, Regno Unito.