CILD Coalizione Italiana Libertà e Diritti civili

RIFORMA ITALIANA SULL'HACKING

Analisi di Privacy International sulla riforma italiana sull'hacking all'interno del DDL Orlando, prima dell'esame della Camera dei Deputati

Sintesi

Privacy International ("PI") è un'organizzazione no-profit e non governativa, con sede a Londra, nel Regno Unito, dedicata alla difesa in tutto il mondo del diritto alla privacy. Fondata nel 1990, PI svolge attività di ricerca ed indagine sulla sorveglianza governativa ed aziendale, con particolare attenzione alle tecnologie che consentono queste pratiche. Per garantire universalmente il rispetto del diritto alla privacy, PI promuove una robusta legislazione a livello regionale, nazionale ed internazionale di tutela del diritto alla privacy. PI ha direttamente iniziato o ha successivamente aderito a procedimenti contenziosi riguardanti il diritto alla privacy nei tribunali degli Stati Uniti, del Regno Unito e dell'Europa, tra cui la Corte Europea dei Diritti dell'Uomo e la Corte di Giustizia Europea. Inoltre PI presta ausilio alle organizzazioni di cui è partner nei paesi in via di sviluppo a rafforzare le proprie capacità di identificare e difendersi da minacce alla privacy. PI si serve di esperti di tecnologia, investigatori, nonché di avvocati che lavorano insieme per comprendere le basi tecniche delle nuove tecnologie di sorveglianza e per studiare in che modo l'attuale impianto normativo possa ad esse applicarsi.

PI si oppone, in via generale, all'attività di hacking ("hacking") come strumento di sorveglianza. Tale posizione è fondata su due preoccupazioni primarie. In primo luogo, l'hacking può essere molto più invasivo di qualsiasi altra tecnica di sorveglianza esistente, inclusa l'intercettazione delle comunicazioni. L'hacking consente ai governi di accedere ai sistemi informatici da remoto e, perciò, a tutte le informazioni memorizzate su tali sistemi. In secondo luogo, ed in modo altrettanto preoccupante, l'hacking è potenzialmente in grado di minare l'integrità non solo del sistema attaccato, ma anche di internet nella sua globalità. Le tecniche di hacking sono fondamentalmente progettate per consentire ad un soggetto non autorizzato di accedere e controllare il sistema di un altro soggetto.
Inoltre, le falle di sicurezza nei sistemi, utilizzate dal governo per consentire

tale controllo, possono anch'esse essere sfruttate da chiunque abbia un'adeguata competenza tecnica.

Nell'esame del sesto rapporto periodico del governo italiano sull'attuazione del Patto Internazionale sui Diritti Civili e Politici, durante la 119° sessione del marzo 2017, il comitato per i diritti umani delle Nazioni Unite ha espresso la propria preoccupazione per l'attività di hacking da parte delle autorità statali:

"Il Comitato è preoccupato circa i report che identificano una diffusa pratica di intercettazione di comunicazioni private e di impiego di tecniche di hacking da parte delle agenzie di intelligence, senza esplicita autorizzazione normativa o in assenza di sufficienti garanzie per evitare abusi... Lo Stato dovrebbe rivedere il sistema normativo delle intercettazioni di comunicazioni private, dell'hacking dei dispositivi digitali e della conservazione dei dati ottenuti al fine di assicurare che:
(a) tali attività siano conformi agli obblighi di cui all'articolo 17 inclusi i principi di legalità, proporzionalità e necessità;
(b) vi sia un robusto sistema di controllo indipendente sui sistemi di sorveglianza, di intercettazione e di hacking, prevedendo anche il coinvolgimento dell'autorità giudiziaria in tutti i casi di autorizzazione di tali misure e consentendo a coloro che le abbiano subite un efficace rimedio in casi di abuso, possibilmente attraverso una notifica ex post sull'assoggettamento a misure di sorveglianza o hacking..." [1]

Mentre il DDL Orlando è un'occasione per colmare l'attuale lacuna legislativa sull'uso dell'hacking per scopi investigativi, PI ritiene che non sia conforme ai requisiti della legge internazionale vigente sui diritti umani.

[1] Osservazioni conclusive del Comitato dei Diritti Umani delle Nazioni Unite sul Sesto Report Periodico Italiano, Doc. CCPR/C/ITA/CO/6, par. 36-37, (28 marzo 2017) (traduzione dall'originale in inglese.)

Background

È stato ampiamente documentato che le autorità italiane abbiano utilizzato malware[2] (indicati come 'Trojan' nel dibattito italiano) al fine di effettuare l'hacking di dispositivi nello svolgimento di indagini penali[3]. Infatti, secondo un recente rapporto "l'utilizzo di malware è il metodo preferito da parte delle autorità investigative in Italia"[4]. Inizialmente i tribunali non hanno ritenuto che la sorveglianza dei dispositivi attraverso l'hacking fosse assimilabile alle

[2] Malware, crasi di malicious software, ovvero software malevolo, si riferisce ad un codice informatico che sia atto a porre in essere azioni su sistemi (come computer, laptop o telefoni cellulari) che non si sarebbero verificate senza il malware stesso. In questo contesto vale la pena distinguere fra l' "exploit" e il "payload", solitamente combinati nel malware. L'exploit sfrutta una vulnerabilità del sistema di sicurezza di un computer o di un'applicazione per permettere l'esecuzione del malware. Il payload è la parte del malware che realizza l'azione sul sistema. Per un ulteriore approfondimento si veda il sommario dell'Amicus Curiae Privacy International a supporto dell'appello del difensore e della decisione, U.S. v. Alex Levin, United States Court of Appeals for the First Circuit, Caso N. 16-1567, pp. 5-8 (10 Febbraio 2017), disponibile al seguente link: https://www.documentcloud.org/documents/3458395-U-S-v-Levin-Privacy-International-Amicus-Brief.html

[3] Per un ulteriore approfondimento si veda: Carola Frediani, Intercettazioni col trojan, ecco la proposta di legge, LA STAMPA (31 Gennaio 2017), disponibile al seguente link: http://www.lastampa.it/2017/01/31/italia/cronache/intercettazioni-col-trojan-ecco-la-proposta-di-legge-MP8BJ2PB0jCwMt84ofRSlM/pagina.html in cui si sottolinea che il Parlamentare Quintarelli abbia detto in una conferenza stampa: "Attualmente gli strumenti sono utilizzati senza uno schema di garanzie e non siamo in grado di determinare quante persone siano soggette a questi strumenti di controllo"; Bill Marczak et. al., "Mapping Hacking Team's "Untraceable" Spyware", in CitizenLab, 17 Febbraio 2017, disponibile al seguente link: https://citizenlab.org/2014/02/mapping-hacking-teams-untraceable-spyware/ in cui si sottolinea che l'Italia è una delle utilizzatrici più prolifiche dei Sistemi di Controllo da Remoto (SCR), uno spyware altamente sofisticato commercializzato solamente nei confronti delle autorità governative da un Team di Hacker milanesi.

[4] Il Framework legislativo in merito all'hacking, Studio commissionato dal Dipartimento per le politiche per i diritti civili e gli affari costituzionali, su richiesta della Commissione LIBE, Marzo 2017, p. 59, disponibile al seguente link: http://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf (d'ora in avanti "Report C del Dipartimento di Policy del Parlamento Europeo")

intercettazioni telefoniche[5]. Di conseguenza, per un hacking di questo tipo non era richiesta un'autorizzazione del giudice per le indagini preliminari, essendo sufficiente, infatti, un'autorizzazione del pubblico ministero[6].

Sentenza della Corte Suprema di Cassazione n. 27100/2015

Nel 2015 la Corte Suprema di Cassazione si è discostata dai suoi precedenti, concludendo che l'hacking da parte della polizia giudiziaria debba essere visto alla stregua della "sorveglianza elettronica" e, quindi, dovrebbe richieda una tradizionale autorizzazione da parte del giudice per le indagini preliminari[7]. In tal modo, la Corte ha sottoposto tale hacking al Codice di Procedura Penale (c.p.p.). L'articolo 266 c.p.p. consente "l'intercettazione di conversazioni o comunicazioni" nei procedimenti relativi ad un elenco di gravi reati specifici. L'articolo 266-bis espande i poteri di sorveglianza autorizzata fino ad includere "l'intercettazione di flussi di comunicazioni relative ai sistemi informatici". Tuttavia, l'art. 266, comma 2, vieta ogni intercettazione effettuata in una casa, in un alloggio o in un altro edificio o struttura di proprietà privata, salvo che non vi sia motivo di credere che l'attività criminosa si sia svolta o si svolga all'interno di tale edificio.

---

[5] Vedi, ad esempio, Corte Suprema di Cassazione, Sez. V, Sentenza n. 24695/2009. Questo caso ha legittimato l'uso di strumenti di hacking per cogliere e copiare i documenti già memorizzati su un dispositivo, in questo caso specifico un disco rigido del computer utilizzato per il proprio lavoro dagli imputati. La Corte si è basata su una falsa caratterizzazione del malware, fondando la decisione su l'errata analisi in cui l'hacking utilizzato solamente per la ricerca di documenti esistenti non comporti l'intercettazione di alcun "flusso di comunicazioni" (come affermato all'articolo 266-bis del Codice di Procedura Penale), e quindi non costituisce un intercettazione telefonica. Il download di tali documenti, ha dichiarato la Corte, implica semplicemente un "rapporto operativo" con il microprocessore, che non rientra nell'intercettazione. La sentenza descrive in modo errato la modalità di sorveglianza basata sull'hacking e ignora anche il potenziale utilizzo di malware per la raccolta di nuovi documenti o per la manipolazione dei dati. La Corte ha ulteriormente appoggiato questo approccio in un caso successivo: Corte suprema di Cassazione, Sez. VI, Caso Bisignani -
Sentenza n. 254865/2012.

[6] Per un ulteriore approfondimento si veda Giuseppe Vaciago e David Silva Ramalho, "Online Searches and Online Surveillance: the Use of Trojans and Other Types of Malware as Means of Obtaining Evidence in Criminal Proceedings", in Digital Evidence and Electronic Signature Law Review Vol. 88, n. 13, 2016, p. 91-92.

[7] Corte Suprema di Cassazione, Sez. VI, Caso Musumeci – Sentenza N. 27100/2015

Sentenza della Corte Suprema di Cassazione (Sezioni Unite) del 2016

Dati i termini di cui all'articolo 266, comma 2, riguardante le intercettazioni in proprietà private, la Corte Suprema di Cassazione, nel 2016, si è nuovamente pronunciata sul tema. La questione su cui si è pronunciata la Corte è se le autorità italiane potessero continuare ad effettuare l'hacking dei dispositivi, dato che tale attività potrebbe fornire all'autorità accesso illimitato all'ambiente circostante in cui si trova il dispositivo (come ad esempio l'abitazione privata), anche in situazioni in cui l'attività illecita non sia stata intrapresa al loro interno, in apparente violazione dell'art. 266, comma 2[8]. La Corte ha riconosciuto diverse modalità di utilizzo del malware, eseguendo così una mappatura delle capacità dell'hacking al fine di includervi: (1) la registrazione di tutto il traffico di dati in entrata o in uscita (ad esempio la cronologia di navigazione, l'utilizzo della posta elettronica, il contenuto delle comunicazioni, la geo-localizzazione, i messaggi di testo e le foto); (2) la possibilità di accendere e spegnere il microfono e la videocamera di un dispositivo, senza che il proprietario ne sia a conoscenza; (3) la ricerca all'interno del disco rigido e la copia di tutto o parte dell'unità di memoria del dispositivo; (4) il decriptaggio di tutto ciò che è stato digitato sulla tastiera, attraverso i key-loggers, e la raccolta di tutto ciò che appare sullo schermo, facendo foto istantanee dello schermo ("screenshot"), indipendentemente dal fatto che il proprietario utilizzi la crittografia o altre tecnologie di sicurezza[9].

La Corte ha rilevato che, alla luce delle minacce alla società poste in essere "dalle articolate organizzazioni criminali che dispongono di sofisticate tecnologie e di notevoli risorse finanziarie" - ed oggi, anche dalla crescente diffusione ed articolazione su scala mondiale delle organizzazioni terroristiche "la vigente legislazione, nonché i principi costituzionali

[8] Corte Suprema di Cassazione, Sezioni Unite, Caso Scurato – Sentenza N. 26889/2016, Svolgimento del Processo, par. 2

[9] Idem, Motivi della decisione, par. 2 (a partire da "uno strumento tecnologico di questo tipo consente lo svolgimento di varie attività e precisamente", a seguito di cui la Corte elenca i vari usi di un malware).

consentono - per adeguare l'efficacia investigativa all'evoluzione tecnologica dei mezzi adoperati dai criminali."[10]. La Corte ha distinto tra due categorie di attività: "la ricerca on-line" e "la sorveglianza online". Mentre la prima contempla la copia di unità di memoria esistenti, la seconda comprende tutte le altre forme di sorveglianza basate sull'hacking. Alla luce di quanto previsto all'articolo 266, comma 2, la Corte ha stabilito che per quanto riguarda "la sorveglianza online" (cioè "l'intercettazione in tempo reale" attraverso il malware) tale attività potrebbe essere lecita ai sensi dell'articolo 266, comma 2, ma deve essere utilizzata "limitatamente ai procedimenti per delitti di criminalità organizzata"[11] (ovvero, i reati connessi alla mafia e al terrorismo). La Corte ha indicato che in tali circostanze "anche nei luoghi di privata dimora ex art. 614 cod. pen., pure non singolarmente individuati e anche se ivi non si stia svolgendo l'attività criminosa - sia consentita l'intercettazione di conversazioni o comunicazioni tra presenti, mediante l'installazione di un "captatore informatico" in dispositivi elettronici portatili (ad es., personal computer, tablet, smartphone ecc.)"[12]. La Corte ha quindi concluso che l'intercettazione effettuata per mezzo di un "apparecchio digitale" installato su un dispositivo portatile sarebbe in linea con l'articolo 266 del codice penale, nonché con la Costituzione e con gli obblighi derivanti dall'articolo 8 della Convenzione europea dei diritti dell'uomo e delle libertà fondamentali, che tutelano il diritto alla privacy[13]. Vale la pena notare che la Corte ha riconosciuto che il giudice per le indagini preliminari che autorizzi le suddette misure non è in grado di prevedere l'entità della possibile intrusione nella dimora del singolo individuo, a seguito dell'immissione del malware, "*con conseguente impossibilità di effettuare un adeguato controllo circa l'effettivo rispetto della normativa che legittima, circoscrivendole, le intercettazioni domiciliari*

[10] Idem, Motivi della decisione, par. 10.1

[11] Idem, Motivi della Decisione, par. 11

[12] Ibidem

[13] Idem, par. 10.2

di tipo tradizionale"[14]. La Corte, tuttavia, non ha ritenuto che tutto ciò fosse in grado di negare il potere di effettuare l'hacking nell'ambito del quadro normativo vigente.

Proposte legislative

Negli ultimi anni sono state presentate quattro diverse proposte legislative che hanno tentato di regolare esplicitamente la sorveglianza attraverso l'hacking[15]. Nessuna di queste proposte ha superato l'esame del Parlamento. Tuttavia ciò che distingueva le due proposte più recenti - l'emendamento "Casson" e il progetto di legge "Quintarelli" – si sostanziava nella differenziazione delle varie capacità dei malware "in quanto il grado di invasività varia in base alla funzione"[16]. Entrambe le proposte, quindi, introducevano una maggiore supervisione, controlli di sicurezza, e procedure di minimizzazione, alla luce delle caratteristiche specifiche dell'hacking, distinte da quelle delle altre attività di sorveglianza.

[14] Idem, par. 6

[15] Come sintetizzato da Giuseppe Vaciago & David Silva Ramalho, nt. 6, p. 92 – 93, "Oltre alle decisioni del caso di specie, durante l'ultimo anno in Italia si sono succeduti quattro progetti di legge per portare lo strumento investigativo nell'ambito del Codice di Procedura Penale: il primo progetto di legge è stato presentato come parte di una nuova legge di risposta alle attività terroristiche. In questo progetto di legge, è stato fatto un tentativo errato per aggiungere all'articolo 266-bis, che disciplina la sorveglianza informatica, la capacità di svolgere tale tipo di attività anche attraverso l'utilizzo di uno strumento o di un software per l'acquisizione remota di comunicazioni e di dati trovati in un sistema informatico. Fortunatamente, questo emendamento è stato criticato da diversi parlamentari e dal primo ministro, in quanto introduceva la possibilità di intraprendere attività estremamente invasive nei confronti dei cittadini senza alcuna garanzia legale diversa dalla mera considerazione di tale strumento come un esempio di sorveglianza elettronica. Lo stesso destino è spettato alla legge "Greco" del 2 dicembre 2015. All'inizio del 2016 sono state elaborate due bozze di legge (emendamento "Casson" e "Quintarelli") con un approccio apparentemente diverso da quello dell'anno precedente."

[16] Report C del Dipartimento di Policy del Parlamento Europeo, supra nota. 4. Per una dettagliata analisi della Proposta Quintarelli si vedano p. 87 – 89. Per un ulteriore approfondimento si veda la Lettera di Access Now diretta a Stefano Aterno, "Re: Disciplina dell'uso dei captatori legali nel rispetto delle garanzie individuali", 29 Marzo 2017, disponibile al seguente link: http://www.civicieinnovatori.it/?page id=211

DDL Orlando

Il 15 marzo 2017, il Senato ha votato un progetto di legge, proposto dal ministro della Giustizia Andrea Orlando, che modifica il Codice di Procedura Penale (di seguito: "DDL Orlando", o "il disegno di legge")[17]. Il disegno di legge è ora in attesa di approvazione da parte della Camera dei Deputati. Il disegno di legge fa parte di una più ampia riforma del sistema giudiziario italiano e comprende l'impegno a modificare l'articolo 268 del Codice di Procedura Penale (la norma che opera e limita l'articolo 266). Nel DDL Orlando, il governo ha il compito di disciplinare (tramite un decreto legislativo) l'hacking per le indagini preliminari. In tal modo, il disegno di legge, come attualmente elaborato, fornisce al governo alcune indicazioni generali su cosa tale decreto debba contenere. Di seguito è riportato il sommario di PI della sezione del disegno di legge relativa all'hacking e l'analisi giuridica della proposta. PI auspica che il testo sia d'aiuto tanto al governo quanto al parlamento nei loro processi consultivi da effettuarsi sia per il disegno di legge che per il potenziale decreto legislativo.

Riepilogo delle disposizioni del DDL Orlando sull'*hacking*

L'articolo 82 del DDL Orlando autorizza il governo ad adottare un decreto legislativo per la riforma delle disposizioni sull'intercettazione delle comunicazioni, in linea con gli orientamenti di cui all'articolo 84. L'articolo 84, lettera e), riguarda la regolamentazione dell'intercettazione delle comunicazioni attraverso i malware ("disciplinare le intercettazioni di comunicazioni tramite immissione di captatori informatici"), ovvero una delle forme di sorveglianza effettuate per tramite l'hacking. Il disegno di legge prevede di offrire 8 linee guida generali relative a tale disciplina (Articolo 84, lettera e), n. 1-8):

[17] Modifiche al codice penale, al Codice di Procedura Penale e all'ordinamento penitenziario, Proposta di Legge, 15 Marzo 2017, disponibile al seguente link: http://www.senato.it/service/PDF/PDFServer/BGT/01009188.pdf

1. L'attivazione del microfono di un dispositivo non avviene automaticamente, e può essere eseguita solo manualmente in conformità con il decreto autorizzativo di un giudice e limitatamente alle istruzioni di cui in detto decreto.

2. Qualsiasi registrazione audio realizzata attraverso tale attivazione deve seguire gli stessi requisiti di registrazione e documentazione di cui all'articolo 268 del Codice di Procedura Penale sulla regolare intercettazione delle comunicazioni, tra cui l'indicazione dell'orario di inizio e fine dell'intercettazione.

3. L'attivazione del dispositivo può essere giustificata per la prevenzione dei reati di cui all'articolo 51 commi 3-bis e 3-quater del Codice di Procedura Penale (in materia di criminalità organizzata, tra cui mafia e terrorismo), o comunque solo in abitazioni dove stia avvenendo un'attività criminosa. In ogni caso, l'autorizzazione del giudice per le indagini preliminari deve indicare le ragioni per le quali è necessario eseguire l'hacking nella conduzione dell'indagine.

4. Tutte le registrazioni devono essere trasferite ad un server controllato dalla procura del pubblico ministero del procedimento, al fine di "garantirne l'originalità e l'integrità". Una volta completata la registrazione, su indicazione della polizia giudiziaria, il malware deve essere disattivato e "reso definitivamente inutilizzabile".

5 Tutti i malware utilizzati per le indagini penali devono essere conformi ai requisiti tecnici stabiliti con decreto ministeriale, da emanare entro trenta giorni dalla data di entrata in vigore del decreto legislativo. Il decreto ministeriale deve tenere costantemente conto dell'avanzamento tecnologico delle tecniche di hacking per assicurare che le operazioni soddisfino "standard idonei di affidabilità tecnica, di sicurezza e di efficacia".

6 Fatte salve le competenze del giudice per le indagini preliminari in casi ordinari, il pubblico ministero può autorizzare l'intercettazione di cui sopra senza previa autorizzazione del giudice in "casi di urgenza". Nel decreto di urgenza, il pubblico ministero deve mostrare le circostanze specifiche che hanno reso impossibile l'iter prestabilito e le ragioni per le quali l'attività di hacking in questione è necessaria per lo svolgimento delle indagini. Il pubblico ministero deve richiedere anche la successiva convalida al giudice per le indagini preliminari entro un lasso di tempo non superiore a 48 ore.

7 La raccolta di informazioni effettuata tramite il malware, originariamente autorizzata per un reato specifico, può essere utilizzata come prova nel perseguimento di altri reati di cui all'articolo 380 del Codice di Procedura Penale (come ad esempio il traffico di stupefacenti o il furto), se in seguito si constatasse che il malware sia "indispensabile" per l'indagine su tali reati.

8 Il disegno di legge riconosce come possibile l'"occasionale" apprensione di dati non inerenti all'indagine di individui non collegati ai fatti oggetto dell'indagine. Il disegno di legge stabilisce una salvaguardia limitata, per cui tali informazioni, se intercettate, non dovrebbero essere rivelate, condivise, o in altro modo rese note.

Analisi giuridica delle disposizioni del DDL Orlando sull'*hacking*

In via preliminare, è importante riaffermare la posizione di Privacy International in opposizione all'hacking come strumento per la sorveglianza. La posizione è fondata su due preoccupazioni primarie. In primo luogo, l'hacking è potenzialmente molto più invadente di qualsiasi altra tecnica di sorveglianza esistente, inclusa l'intercettazione delle comunicazioni. L'hacking consente alle autorità statali di accedere ai sistemi da remoto e quindi a tutte le informazioni memorizzate su tali sistemi. Inoltre, un numero crescente di dispositivi che compongono il c.d. "Internet delle cose" - come un frigorifero che registra quando e quale persona mangia o una televisione che registra ciò che una persona guarda e le sue reazioni - documentano dettagli intimi sulle vite delle persone. Accedendo a queste informazioni, le autorità statali possono acquisire una profonda e completa conoscenza della vita di un individuo, rivelandone l'identità, i pensieri, le relazioni, gli interessi e le attività. L'hacking consente anche il controllo da parte delle autorità sulla funzionalità dei sistemi, come è stato discusso in precedenza, e consente quindi il monitoraggio completo e continuo della vita di una persona. Le intrusioni nella privacy tramite l'hacking governativo sono enormemente amplificate se oggetto delle stesse sia un'infrastruttura di rete (come nel caso dell'hacking di un server DNS utilizzato da un'impresa, con cui si può accedere ai sistemi di tutti gli utenti del server, ovvero i dipendenti della stessa).

In secondo luogo, altrettanto preoccupante è il fatto che l'hacking abbia il potenziale di minare l'integrità non solo del sistema attaccato, ma anche della Rete internet nel suo complesso. Le tecniche di hacking sono fondamentalmente progettate per consentire a una parte non autorizzata di accedere e controllare il sistema di un'altra parte.

Lo stratagemma utilizzato dal governo per eludere la sicurezza dei dispositivi può essere sfruttato da chiunque abbia le pertinenti competenze tecniche.

Certamente le autorità statali non possono mai giustificare l'affidamento all'hacking come "metodo prescelto", come, invece, sembra suggerire che accada in Italia sulla base della relazione della commissione del Parlamento europeo per le libertà civili, la giustizia e gli affari interni (LIBE)[18]. Il relatore speciale delle Nazioni Unite sulla libertà di espressione ha ulteriormente rilevato che:

"I software di intrusione offensivi come i Trojan o la capacità di intercettazione di massa costituiscono una sfida alle nozioni tradizionali di sorveglianza che non possono essere riconciliate con le leggi vigenti sulla sorveglianza e l'accesso alle informazioni private. Non esistono solo nuovi metodi per effettuare la sorveglianza, ma anche nuove forme di sorveglianza. Dalla prospettiva dei diritti umani l'uso di tali tecnologie è estremamente inquietante"[19].

Ciò è particolarmente vero in considerazione del fatto che una delle ratio fondamentali di precedenti progetti di legge in merito all'hacking in Italia è stata quella di fornire agli investigatori statali la capacità di eludere le tecnologie di crittografia[20]. Come evidenziato nella proposta "Quintarelli", per esempio, "la crittografia impenetrabile" ha permesso agli utenti di poter effettuare comunicazioni che risultano non raggiungibili da parte della polizia giudiziaria.

[18] Supra, nt. 4

[19] Supra, nt. 1

[20] Ad. Es. La proposta di legge "Quintarelli", Disciplina dell'uso dei captatori legali nel rispetto delle garanzie individuali, Preambolo 2, n. 1-ter. Il testo della proposta è disponibile al seguente link: http://www.civicieinnovatori.it/wp-content/uploads/2017/02/Sintesi-PDL-captatori-EN.pdf

È in questo contesto che l'hacking è percepito come uno strumento desiderabile per le autorità investigative nonostante indebolisca la sicurezza che gli individui possano godere online[21].

Le preoccupazioni generali espresse nei precedenti paragrafi dimostrano come la regolamentazione dei poteri di hacking attraverso lo strumento legislativo sia un primo passo necessario, anche perché le autorità italiane hanno già utilizzato le funzionalità dell'hacking senza espressa autorizzazione ex lege, come ha giustamente criticato il Comitato per i Diritti Umani delle Nazioni Unite[22]. Pertanto, con tale disciplina l'Italia muove un passo in avanti verso il raggiungimento dei requisiti richiesti dal diritto internazionale in materia di diritti umani. Detto questo, il disegno di legge soffre di una serie di deficit strutturali e manca di procedure di salvaguardia e minimizzazione, che lo rendono, nella forma attuale, incompatibile con gli obblighi internazionali in materia di diritti umani.

PI vuole portare all'attenzione del Parlamento e dell'esecutivo le seguenti dieci questioni chiave:

[21] U.N. Risoluzione del Consiglio dei diritti umani sulla sicurezza dei giornalisti, U.N. Doc. A / HRC / 33 / L.6 (26 settembre 2016). La risoluzione sottolinea che, nell'era digitale, gli strumenti di crittografia e anonimato sono diventati vitali per molti giornalisti per esercitare liberamente il proprio lavoro ed il proprio godimento dei diritti umani, in particolare i loro diritti alla libertà d'espressione e alla privacy, anche per assicurare le comunicazioni e per proteggere la propria riservatezza ed invita gli Stati a non interferire con l'uso di tali tecnologie, evitando qualsiasi restrizione che infranga gli obblighi degli stessi in forza del diritto internazionale in materia di diritti umani); Relazione del relatore speciale sulla promozione e la tutela del diritto alla libertà di opinione e d'espressione, U.N. Doc. A / HRC / 29/32 (22 Maggio 2015) "Gli Stati non dovrebbero limitare la crittografia e l'anonimato, che facilitano e a volte esplicano in sé il diritto alla libertà di opinione e di espressione. La restrizioni globali non sono necessarie e proporzionate. Gli Stati dovrebbero evitare tutte le misure che indeboliscano la sicurezza che i singoli possono godere on-line, come standard deboli di crittografia, "backdoors" e "key escrows".

[22] Supra, nt. 1

1. Principio di legalità

Come precisato dall'Assemblea Generale delle Nazioni Unite, "la sorveglianza delle comunicazioni digitali deve essere coerente con gli obblighi internazionali in materia di diritti umani e deve essere condotta sulla base di un quadro giuridico che deve essere accessibile al pubblico, chiaro, preciso, completo e non discriminatorio"[23].

Al centro del principio di legalità si erge il seguente importante assunto: la proposta di inserire "regimi di sorveglianza intrusivi all'interno delle previsioni normative" deve essere accompagnata "da un dibattito pubblico e parlamentare"[24].

È in questo contesto che i mezzi con cui sono state approvate le disposizioni relative all'hacking nel disegno di legge nel Senato sollevano preoccupazioni. Tali disposizioni sono state frettolosamente redatte e incorporate in una più ampia iniziativa di riforma della giustizia attesa da anni. Successivi emendamenti o un attento dibattito alla Camera, dunque, sembrano improbabili alla luce di questo processo.

Inoltre, la scelta del decreto delegato, per cui il Parlamento si limita ad enunciare le linee guida generalizzate mentre l'esecutivo si occupa di inserire tali orientamenti nelle disposizioni operative (libero da qualsiasi controllo parlamentare aggiuntivo) non è soddisfacente.

Per quanto riguarda il requisito della prevedibilità, l'Italia è tenuta a definire in modo chiaro e limitato le condizioni in cui le capacità dell'hacking possono

[23] Risoluzione dell'Assemblea generale delle Nazioni Unite sul Diritto alla Privacy nell'era digitale, U.N. Doc A/RES/69/166, 18 dicembre 2014

[24] Report del Relatore Speciale sulla promozione e la protezione dei Diritti umani e delle libertà fondamentali nelle more del contrasto al terrorismo, U.N. Doc. A/HRC/34/61, par. 36, 21 febbraio 2017

essere utilizzate[25]. L'ambito di applicazione del progetto di legge non è chiaro e lascia significative lacune normative.

a Oggetto della disciplina. Il disegno di legge si applica alle indagini preliminari avviate dal pubblico ministero e condotte dalla polizia giudiziaria ai sensi del Codice penale. A questo proposito il disegno di legge esclude l'*hacking* effettuato dai servizi segreti italiani, vale a dire l'Agenzia Informazioni e Sicurezza Esterna (AISE), l'Agenzia Informazioni e Sicurezza Interna (AISI), e il Reparto Informazioni e Sicurezza (RIS). È stato riportato che i servizi di intelligence italiani hanno ripetutamente utilizzato l'*hacking* in passato[26].

[25] Si veda Leander contro Svezia, App. N. 9248/81, Corte Europea dei Diritti dell'Uomo, sentenza, par. 51 (26 Marzo 1987) ("Tuttavia, il requisito della prevedibilità nel contesto speciale di controlli segreti del personale
in settori che incidono sulla sicurezza nazionale non possono essere uguali a quelli di tanti altri settori. Ciò non può significare che un soggetto debba essere in grado di prevedere esattamente quali controlli verranno effettuati al riguardo dalla servizio speciale di polizia svedese al fine di proteggere la sicurezza nazionale. Tuttavia, in un sistema applicabile a tutti i cittadini, come nell'ambito dell'Ordinanza di Controllo del Personale, la legge deve essere sufficientemente chiara nei termini da dare una adeguata indicazione delle circostanze in cui e le condizioni alle quali le autorità pubbliche possono ricorrere a questo tipo di segreti ed a tali, potenzialmente, pericolose interferenze con la vita privata. Per valutare se il criterio della prevedibilità è soddisfatto, si possono prendere anche delle istruzioni o prassi amministrative che non hanno lo status di diritto sostanziale, nella misura in cui le persone interessate siano rese sufficientemente consapevoli del loro contenuto. Inoltre, quando l'attuazione della legge consiste in attività segrete non aperte al controllo da parte degli individui o del pubblico in generale, la stessa legge, contrariamente alla prassi amministrativa di accompagnamento, deve indicare la portata di ogni discrezione conferita all'autorità competente con sufficiente chiarezza, tenuto conto del legittimo scopo della misura in questione, per dare all'individuo un'adeguata protezione contro interferenze arbitrarie").

[26] Si veda ad es. Pierluigi Paganini, "Italian intelligence is planning to invest in solutions that could allow its counterterrorism agents to monitor Sony's PlayStation Network", in Security Affairs, 30 Novembre 2015, disponibile al seguente link: http://securityaffairs.co/wordpress/42397/hacking/italian-intelligence-monitoring-playstation.html o "Italian Intelligence Agency Steals Sensitive Info from Indian Embassy", in The Indian Express, 30 July 2011, disponibile al seguente link: http://archive.indianexpress.com/news/italian-intelligence-agency-steals-sensitive-info-from-indianembassy/824712/

Una attività di *hacking* al di fuori di una precisa legislazione non deve essere ammessa, poiché verrebbe eseguita in contraddizione con il principio di legalità. A questo proposito è importante chiarire che la Corte Europea dei Diritti dell'Uomo ha affermato nella sentenza *Liberty vs. Regno Unito*, che non v'è alcuna ragione di applicare diversi livelli di protezione tra organi di polizia e agenzie di intelligence[27].

b Ambito di applicazione della disciplina. La proposta di legge corrente affronta solo un aspetto dell'hacking (l'uso del "payload"[28]) e ne contempla solo un utilizzo (l'attivazione del microfono). La proposta tace per quanto riguarda l'utilizzo del "payload" per altri scopi (come quelli elencati nella sentenza del 2016 della Corte Suprema di Cassazione[29]). Ancora una volta conviene ripetere che l'hacking, comprese le varie funzionalità di un malware, che non sia espressamente disciplinato, viola il principio di legalità e dovrebbe essere proibito. Inoltre all'interno della proposta non sono enunciate linee guida relative agli altri aspetti delle attività di hacking, fra cui i metodi di diffusione dei malware (ad es. gli attacchi di social engineering[30], o gli exploit zero-day[31]) né affronta altri possibili impieghi dei malware nel corso della sorveglianza on-line, come compreso dalla Corte di Cassazione.

---

[27] Corte Europea dei Diritti dell'Uomo, Appello n. 58243/00, Liberty et Al. Vs Regno Unito, Sentenza, par. 63, 1 Luglio 2008

[28] Supra, nt. 2

[29] Supra, nt. 9

[30] Il social engineering implica l'ingannare un soggetto nell'esecuzione di un'azione specifica, come la rivelazione di un nome utente o di una password, per compromettere la sicurezza di un sistema destinatario e consentirne l'accesso non autorizzato. Una tecnica piuttosto comune di social engineering è chiamata phishing, che corrisponde all'invio di una e-mail ad un utente fingendo di essere una persona conosciuta od un'organizzazione, al fine di ottenere informazioni riservate. Le email di phishing possono anche contenere un collegamento o un allegato infettato da un malware, che viene installato sul sistema di destinazione una volta cliccato dall'utente.

[31] Un "exploit zero-day" è un applicativo sconosciuto al software originario.

c Ambito di applicazione temporale del regolamento. Ai sensi dell'articolo 267, comma 3 del Codice di Procedura Penale, l'intercettazione delle telecomunicazioni può essere autorizzata per un massimo di 15 giorni, con la possibilità di prorogarla di due settimane alla volta. Tali proroghe possono continuare senza limiti (il che significa che non c'è un limite massimo complessivo di proroghe), né vi sono requisiti specifici di legge che le autorità investigative debbano presentare per il prolungamento delle intercettazioni. Nel disegno di legge sembrerebbero applicarsi mutatis mutandis queste stesse disposizioni anche ai poteri di hacking concessi alla polizia giudiziaria[32]. Considerando l'intrusività dell'hacking, tali periodi sono sproporzionatamente ampi e non possono essere giustificati. Inoltre, il disegno di legge stabilisce un periodo inferiore per la convalida dell'hacking in "casi di urgenza" rispetto a quello che esiste per le intercettazioni ai sensi dell'articolo 267, comma 2. Considerando che, per quest'ultimo caso, al giudice per le indagini preliminari deve essere notificato entro 24 ore il decreto motivato che dispone le intercettazioni (e conseguentemente il giudice avrà 48 ore per convalidarlo), in base al progetto di legge, i decreti del pubblico ministero verso il giudice per i "casi di urgenza" possono essere effettuati entro 48 ore. Considerando anche il fatto che sia il codice che il disegno di legge non identificano quali siano i "casi di urgenza", il disegno non soddisfa lo standard di legalità suddetto[33].

[32] Incorporando i poteri di hacking all'interno delle disposizioni regolamentari che regolano l'intercettazione tradizionale.

[33] Per i motivi discussi, l'ambito temporale del regolamento non soddisfa neanche gli standard di necessità e proporzionalità. Gli standard sono descritti in dettaglio in seguito.

2. Extraterritorialità

Il disegno di legge non precisa espressamente il suo ambito territoriale di applicazione[34]. È quindi soggetto ad interpretazione quando un giudice possa autorizzare l'hacking dei dispositivi al di fuori del territorio italiano. In conformità con il diritto internazionale, la giurisdizione per le attività investigative è limitata dalla sovranità territoriale dello Stato estero[35]. Gli strumenti principali in questi casi sono i Trattati Di Reciproca Assistenza Giudiziaria (Mutual Legal Assistance Treaty "MLAT"), vale a dire quei meccanismi previsti negli stessi trattati che facilitano la cooperazione tra polizie giudiziarie e l'assistenza a sostegno di un'indagine o un procedimento penale in corso[36]. Il relatore speciale delle Nazioni Unite David Kaye ha sottolineato che: "l'incapacità del regime derivante dai trattati di reciproca assistenza giudiziaria a tenere il passo con le richieste di dati transfrontaliere, può condurre gli Stati membri a ricorrere a misure invasive di sorveglianza extraterritoriali"[37].

[34] Questa mancanza inerisce direttamente il principio di legalità, ma solleva anche ulteriori problematiche.

[35] S.S. Lotus (Francia / Turchia), 1927 P.C.I.J. (Ser. A), n. 10, pp. 18-19 "Ora la prima e più importante restrizione imposta dal diritto internazionale ad uno Stato è che in mancanza di un previsione contraria, esso non può esercitare il suo potere in nessuna forma nel territorio di un altro Stato. In questo senso la giurisdizione è certamente territoriale; il potere di uno Stato non può essere esercitato al di fuori del proprio territorio se non in virtù di una norma derivante dagli usi internazionali o da una convenzione"; International Bar Association, Report of the Task Force on Extraterritorial Jurisdiction, pag. 10 (2009), la quale rileva che "uno Stato non può investigare su un crimine, arrestare un sospetto o far valere una propria sentenza o un processo giudiziario nel territorio di un altro Stato senza ottenere l'autorizzazione".

[36] Ahmad Ghappour, "Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web", in Stan. L. Rev. n. 20 in corso di pubblicazione, 2017.

[37] Report del Relatore Speciale sulla promozione e la protezione del diritto alla libertà di opinione ed espressione, U.N. Doc. A/HRC/32/38, par. 61, 11 Maggio 2016

Uno Stato non dovrebbe aggirare il processo derivante dal MLAT, ma piuttosto aggiornarlo per renderlo efficace nell'era digitale[38].In tema di dispositivi utilizzanti le tecnologie per l'anonimato ciò è particolarmente preoccupante, dato che le forze dell'ordine di alcuni paesi ritengono che "per i soggetti anonimi non rilevi la territorialità in tutte le fasi delle indagini, al fine di evitare la necessità di dover far ricorso ai trattati di reciproca assistenza[39].

[38] Cfr. Ad es., U.N. Consiglio di sicurezza Ris. 2322, Minacce alla Pace e alla Sicurezza Internazionale causate dagli attentati terroristici, U.N. Doc. S / RES / 2322, OP13 (B) (2016) "La relazione invita tutti gli Stati a: ...(b) adottare e, se del caso, riesaminare e aggiornare le leggi in materia di estradizione e mutua assistenza legale in relazione a reati legati al terrorismo, in linea con i propri obblighi internazionali, compresi quelli derivanti dai diritti umani internazionali, e di prendere in considerazione la revisione delle leggi e dei meccanismi nazionali di assistenza legale in materia di terrorismo e l'aggiornamento delle stesse come necessario, al fine di rafforzarne l'efficacia, in particolare alla luce del sostanziale aumento del volume di dati digitali richiesti"

[39] Ghappour, supra nt. 36, p. 20 - 21

3. Necessità e proporzionalità[40]

Il disegno di legge autorizza la misura consistente nell'attivazione del microfono non solo nei casi di minacce perpetrate dalla criminalità organizzata contro l'integrità dello stato (il terrorismo e la mafia), ma anche per altri reati (fintanto che vengano commessi all'interno di un'abitazione).

L'hacking, qualora sia autorizzato, deve essere limitato solo ai crimini più gravi, punto fermo della decisione della Corte Suprema di Cassazione del 2016[41].

Inoltre, il disegno di legge soffre di una serie di carenze che non rispettano i principi di necessità e proporzionalità.

In particolare:

a Il disegno di legge non fissa un limite per cui l'*hacking* possa essere utilizzato solo in presenza di un'assoluta necessità nella conduzione dell'indagine, previo esaurimento di tutti i mezzi di prova meno invasivi previsti. Il disegno di legge non stabilisce ulteriori standard per valutare le informazioni captate, rilevanti e necessarie al fine di giungere a sospetti tali da giustificare l'attività di *hacking*.

b Il progetto di legge consente l'utilizzo a fini probatori di dati relativi ad altri reati, diversi da quelli che costituivano il presupposto

---

[40] U.N. Diritti Umani, Commento generale n. 16: Articolo 17 (Diritto alla Privacy), U.N. Doc. HRI/GEN/1/Rev. 1, p. 21, 8 Apr. 1988, "L'espressione "interferenza arbitraria" è anche rilevante per la protezione del diritto previsto dall'articolo 17. Secondo il Comitato l'espressione "interferenza arbitraria" può anche estendersi all'interferenza prevista dalla legge. L'introduzione del concetto di arbitrarietà ha lo scopo di garantire anche questo,
ovvero che le interferenze previste dalla legge dovrebbero essere conformi alle disposizioni, agli obiettivi dell'Alleanza e dovrebbe essere, in ogni caso, ragionevole in circostanze particolari"; Digital Rights Ireland Ltd. vs. Minister of Communications, Marine and Natural Resources et al. (C-293/12); Kärntner Landesregierung et al. (C-594/12), Casi congiunti, Corte di giustizia dell'Unione Europea, Grande Camera, Sentenza, 8 Aprile 2014, "Secondo la costante giurisprudenza della Corte, il principio di proporzionalità richiede che gli atti delle istituzioni dell'UE siano appropriati per il conseguimento degli obiettivi legittimi perseguiti dalla legislazione in questione e non devono superare i limiti di ciò che è appropriato e necessario per conseguire tali obiettivi"

[41] Supra, nt. 11

dell'autorizzazione, raccolti incidentalmente all'interno di un'operazione autorizzata. Ciò potrebbe incentivare un uso eccessivamente ampio dell'*hacking*, al fine di catturare attraverso tale mezzo informazioni rilevanti per indagini diverse. Le informazioni recepite per il tramite dell'*hacking* devono essere utilizzate solo per gli scopi per cui sono state raccolte, in base al mandato, in modo da ridurre al minimo l'accesso alle informazioni irrilevanti e non pertinenti.

c Il disegno di legge non stabilisce alcun limite circa il metodo, l'estensione e la durata delle operazioni di *hacking* proposte.

d Il disegno di legge non riconosce i potenziali rischi ed i danni per la sicurezza e l'integrità del sistema oggetto di sorveglianza e dell'infrastruttura internet in generale; né come tali rischi e danni possano essere mitigati o corretti, in modo da consentire una valutazione della proporzionalità della misura di *hacking* rispetto alle implicazioni sulla sicurezza.

e Il disegno di legge fa riferimento vago all'intercettazione "occasionale" di comunicazioni relative a soggetti innocenti. Il disegno di legge stabilisce solamente una protezione limitata, in base alla quale tali informazioni non devono essere condivise. Qualsiasi raccolta di dati collaterali deve essere considerata alla luce del principio di proporzionalità, e tale considerazione deve essere introdotta nella disciplina normativa. Inoltre, in caso di raccolta accidentale, occorre introdurre una maggiore protezione, ad esempio attraverso l'obbligo di eliminare immediatamente le informazioni irrilevanti raccolte. A questo proposito è importante chiarire che tutte le operazioni di *hacking* devono essere mirate e basate su un ragionevole sospetto[42], e che l'accesso alla raccolta dei dati ed anche alle comunicazioni incidentali, deve essere mitigato nella misura più ampia possibile.

f Particolare importanza dovrebbe essere data alle persone le cui comunicazioni sono suscettibili di essere oggetto di segreto professionale o immunità ai sensi della legge italiana. Ciò include giornalisti, avvocati, giudici, medici, operatori sociali, piscologi/psicoterapeuti e psichiatri, membri del clero, parlamentari e diplomatici. Il disegno di legge non fornisce ulteriori tutele per i dispositivi e le informazioni di questi soggetti[43].

[42] Si veda ad es. Roman Zakharov v. Russia, Appello N. 47143/06, Corte Europea dei Diritti dell'Uomo, Sentenza, par. 260, 4 Dicembre 2015, "Volgendo ora lo sguardo allo scopo della revisione delle autorità autorizzante, la Corte ribadisce che essa deve essere in grado di verificare l'esistenza di un ragionevole sospetto nei confronti dell'interessato, in particolare, se ci sono indicazioni di fatto per sospettare che la persona pianifichi, di commetta o di abbia commesso atti criminali o altri atti che possano dare luogo a misure di sorveglianza in incognito, come ad esempio atti che mettano in pericolo la sicurezza nazionale. Deve inoltre accertare se l'intercettazione richiesta soddisfi il requisito di «necessità in una società democratica», come previsto dall'articolo 8 § 2 della Convenzione, anche se si tratta di misura proporzionata agli obiettivi perseguiti, verificando, ad esempio, se sia possibile raggiungere gli obiettivi con mezzi meno restrittivi"

[43] Si veda ad es. Kopp v. Switzerland, Appello N. 23224/94, Corte Europea dei Diritti dell'Uomo, Sentenza, par. 71 – 75, 25 Marzo 1998, riguardante la sorveglianza sugli avvocati ; U.N. Doc. A/HRC/29/32, supra nt. 21, par. 59, 22 Maggio 2015, riguardante la sorveglianza sui giornalisti e gli attivisti per i diritti umani.

4. Autorizzazione giudiziaria

Come ha osservato la Corte Europea dei Diritti dell'Uomo nel caso Klass vs. Germania, già nel 1978:

"Il riesame sul provvedimento sulla sorveglianza può intervenire in tre fasi: quando è commissionata, mentre è svolta o quando giunge al termine. Per quanto riguarda le prime due fasi, la stessa natura e la logica della sorveglianza segreta impongono che non solo la sorveglianza in sé ma anche la il riesame accompagnatorio, siano effettuati senza che l'individuo ne sia a conoscenza. Di conseguenza, poiché l'individuo sarà necessariamente impedito nel cercare un effettivo rimedio di propria iniziativa o nel partecipare direttamente a qualsiasi procedura di ricorso, è essenziale che le procedure stabilite forniscano di per sé garanzie adeguate ed equivalenti a salvaguardare i diritti dell'individuo. Inoltre, i valori di una società democratica ed il limite della necessità devono essere pedissequamente seguiti nelle procedure di riesame, ai sensi dell'articolo 8, paragrafo 2, evitandone l'elusione. Uno dei principi fondamentali di una società democratica è il principio di legalità, espressamente menzionato nel preambolo della Convenzione. Il principio di legalità implica, tra l'altro, che un'interferenza da parte delle autorità esecutive nei diritti di un individuo dovrebbe essere soggetta ad un controllo efficace, il quale dovrebbe normalmente essere garantito dall'autorità giudiziaria, almeno in ultima istanza, offrendo le migliori garanzie di indipendenza, imparzialità e una procedura corretta."[44]

La proposta di legge sollecita solamente la polizia giudiziaria a chiedere un mandato in un caso di attivazione del microfono. È importante ribadire che qualsiasi altra operazione di hacking, non prevista dalla legge e non ulteriormente autorizzata da un giudice, dovrebbe essere vietata. Questo approccio è in linea con il consolidato orientamento sia del Comitato per i

[44] Klass and Others v. Germany, Appello N. 5029/71, Corte Europea dei Diritti dell'Uomo, Sentenza, par. 55, 6 Settembre 1978

Diritti Umani delle Nazioni Unite che della Corte Europea dei Diritti dell'Uomo (ECtHR) che richiede un mandato specifico per qualsiasi attività di sorveglianza[45].

Inoltre, il disegno di legge come attualmente elaborato sollecita solo le autorità a fornire al giudice le informazioni sui "motivi per cui l'hacking sia necessario ai fini dell'inchiesta". Questa formulazione non copre tutte le informazioni necessarie al giudice per valutare il provvedimento sulla base dei principi di necessità e di proporzionalità, valutazione che non è neanche contemplata direttamente nell'attuale disegno di legge. Prima di qualsiasi operazione di hacking, l'autorità deve, almeno, stabilire con un alto grado di probabilità che:

- è stato o sarà commesso un grave reato;
- il sistema oggetto dell'operazione contiene informazioni pertinenti e necessarie in merito ai gravi reati o atti costituenti una minaccia specifica per il presunto interesse di sicurezza nazionale;
- le prove pertinenti e necessarie all'indagine su atti o reati gravi saranno ottenute tramite l'hacking del sistema oggetto di sorveglianza.

La richiesta di un mandato deve quindi essere specifica e mirata, e fornire informazioni concrete sull'identità della persona che utilizza il sistema, la sua posizione e altri dettagli identificativi relativi al sistema[46]. La richiesta di un mandato deve anche fornire le informazioni relative ai metodi da impiegare e la portata della loro intrusione nel sistema di destinazione.

[45] Si veda ad es. Osservazioni conclusive sulla quarta relazione periodica sulla Repubblica di Corea, Comitato per i Diritti Umani, U.N. Doc. CCPR/C/KOR/CO/4, par. 43, 3 Dicembre 2015; Association for European Integration and Human Rights and Ekimdzhiev vs. Bulgaria, Appello N. 62540/00, Corte Europea dei Diritti dell'Uomo, Sentenza, par. 85-88, 28 Giugno 2007

[46] Supra, nt. 42

Le richieste di tali mandati potrebbero includere informazioni di carattere tecnico ed i giudici che esaminano tali richieste devono perciò essere in grado di consultare consulenti tecnici competenti sulle tecnologie pertinenti all'indagine. Il disegno di legge come attualmente elaborato non affronta questa tematica.

5. Conservazione e distruzione delle informazioni

Sulla questione della distruzione delle informazioni ottenute, la Corte Europea dei Diritti dell'Uomo ha stabilito, nel caso Weber e Saravia vs Germania, che:

"La distruzione dei dati personali non appena essi non siano più necessari per conseguire il loro scopo e [...] la verifica, a intervalli regolari e ragionevolmente brevi, di quanto siano soddisfatte le condizioni di tale distruzione costituiscono un importante elemento nel ridurre gli effetti dell'interferenza con il segreto delle telecomunicazioni al minimo inevitabile" [47]

Il disegno di legge ignora queste importanti salvaguardie, non stabilendo alcun obbligo sui mezzi con cui i dati raccolti dall'attività di hacking devono essere conservati o distrutti. Il disegno stabilisce solo che, una volta che l'operazione di hacking è cessata, il malware deve essere disattivato "e reso permanente inoperabile". Tuttavia, il disegno di legge non affronta la questione della conservazione e della distruzione delle informazioni raccolte dal malware. Il disegno deve precisare che ogni informazione irrilevante o non pertinente ottenuta in virtù di un'operazione autorizzata deve essere immediatamente distrutta, e che le informazioni pertinenti e rilevanti ottenute da un hacking dovrebbe essere mantenuta con chiare limitazioni temporali. Infine, il disegno di legge dovrebbe chiarire se qualsiasi condivisione di informazioni derivante dall'hacking con altri corpi di forze dell'ordine o autorità straniere sia soggetta agli stessi framework normativi che disciplinano le altre forme di sorveglianza.

[47] Weber e Saravia vs. Germany, Appello N. 54934/00, Corte Europea dei Diritti dell'Uomo, Pronuncia sull'ammissibilità, par. 132, 29 Giugno 2006

6. Trasparenza e supervisione

Uno dei componenti chiave della risoluzione dell'Assemblea Generale delle Nazioni Unite sul diritto alla privacy nell'era digitale, adottata a unanimità, riguarda la salvaguardia della trasparenza e della supervisione.

La risoluzione invita tutti gli Stati:

"Ad istituire o a mantenere gli esistenti meccanismi di supervisione domestica in campo giudiziale, amministrativo e/o parlamentare garantendone l'indipendenza, l'efficacia, e la disposizione di risorse adeguate, affinché assicurino la trasparenza, a seconda dei casi, e la responsabilità dello Stato per la sorveglianza delle comunicazioni, per la loro intercettazione e per la raccolta dei dati personali." [48]

Il disegno di legge come attualmente elaborato non stabilisce obblighi specifici per la divulgazione delle informazioni, anche in forma aggregata, relative alle richieste di hacking da parte delle forze dell'ordine e delle agenzie di intelligence italiane. Il disegno di legge, inoltre, non stabilisce alcun specifico meccanismo di revisione ex post (giudiziario, amministrativo o parlamentare), né ulteriori protezioni dall'abuso di questo potere, che possano rendere il controllo del pubblico maggiormente penetrante. Tali questioni devono essere risolte prima di poter utilizzare l'hacking.

[48] U.N. Doc A/RES/69/166, supra nt.23, par. OP4

Come ha rilevato l'Alto Commissario delle Nazioni Unite per i diritti umani:

"La mancanza di un controllo efficace ha contribuito ad una mancanza di responsabilità riguardo le intrusioni arbitrarie o illecite sul diritto alla privacy nell'ambiente digitale. Le tutele interne senza controllo esterno e indipendente, in particolare, si sono dimostrate inefficaci contro i metodi di sorveglianza illeciti o arbitrari.Mentre queste misure di sicurezza possono assumere una varietà di forme, il coinvolgimento di tutti i rami delle forze dell'ordine nella supervisione dei programmi di sorveglianza, nonché la presenza di un'agenzia indipendente di sorveglianza civile, sono essenziali per garantire l'effettivo rispetto della legge." [49]

[49] Relazione dell'Ufficio dell'Alto Commissario per i diritti umani delle Nazioni Unite, "Il diritto alla privacy nell'era digitale", U.N. Doc. A/HRC/27/37, par. 37, 30 Giugno 2014

7. Sicurezza e integrità dei sistemi

Il disegno di legge deve vietare espressamente l'indebolimento della sicurezza e dell'integrità dei dispositivi e/o sistemi. A questo proposito è preoccupante che il disegno di legge ignori il metodo di propagazione dei malware, in particolare, quando le forze dell'ordine possano utilizzare gli exploit (compresi gli "zero-day exploit"[50]) per effettuare l'hacking di un dispositivo. Nella misura in cui tali tipi di strumenti sono ammessi, è necessario considerare che possono avere un impatto negativo sulla sicurezza e sull'integrità dei dispositivi e dei sistemi oggetto di sorveglianza, in quanto sfruttano le falle nella sicurezza potendo estendere i propri effetti anche a dispositivi e, a sistemi diversi da quello target. Inoltre, alcuni metodi di diffusione, come ad esempio il watering hole (con cui si installa il malware su un sito web, per poi sfruttare le debolezze di dispositivi che accedono al sito), sono per default indiscriminati, e dovrebbero pertanto essere esplicitamente vietati[51]. La mancanza di una regolamentazione sul metodo di diffusione costituisce quindi un problema significativo.

Il Preambolo della Convenzione del Consiglio d'Europa sulla criminalità informatica, di cui l'Italia è uno Stato membro, stabilisce che "è necessario scoraggiare ogni azione diretta contro la riservatezza, l'integrità e la disponibilità dei sistemi, delle reti e dei dati informatici, nonché l'abuso di tali sistemi, reti e dati". Sarebbe una sfortunata conseguenza se se, nel tentativo di difendere l'integrità e la sicurezza dei sistemi (combattendo contro gli atti di terrorismo sia informatico che non), il governo italiano sviluppasse e impiegasse strumento tali da causare gli stessi effetti.

L'introduzione, nel disegno di legge, di prevedere, in futuro, un decreto ministeriale con il quale le operazioni soddisfino "idonei standard di affidabilità tecnica, sicurezza ed efficacia", sarebbe un ipotesi

[50] Supra, nt. 31

[51] Per un approfondimento si veda supra nt. 2

gradita. Tuttavia, il disegno di legge fa molto poco per offrire una guida significativa sul contenuto del suddetto decreto e sul metodo con cui i malware non siano utilizzati per porre in pericolo la sicurezza e l'integrità dei sistemi.

8. Integrità delle informazioni

La legge non vieta espressamente la manomissione o la modifica dei dati sul dispositivo oggetto dell'hacking. Il disegno di legge deve precisare che i mandati emessi a norma della sua disciplina devono permettere solo la raccolta passiva di informazioni, e non la loro manipolazione o cancellazione. Inoltre, colui che è oggetto di hacking autorizzato deve essere informato, come vedremo di seguito, sul metodo e la portata di hacking, compresi tutti i software utilizzati, in modo che possa comprendere la natura delle informazioni ottenute e indagare su eventuali alterazioni e omissioni delle informazioni o violazioni nella modalità di custodia, a seconda dei casi.

Il fatto che il disegno di legge introduca l'obbligo per cui "tutte le registrazioni devono essere trasferite a un server controllato dalla procura al fine di garantirne l'originalità e l'integrità" è una norma utile. Tuttavia, il disegno di legge deve stabilire restrizioni sull'accesso e garanzie procedurali, per assicurare che solo personale qualificato e preparato possa accedere ai dati ottenuti ed esclusivamente per gli scopi autorizzati dal mandato.

9. Notifica

Il disegno di legge non richiede alcuna notifica alla persona o agli enti, o ad altri utenti identificabili di un sistema posto sotto sorveglianza. L'assenza di questo requisito è in contrasto con gli standard internazionali sui diritti umani, come sottolineato dal relatore speciale delle Nazioni Unite sulla libertà di opinione e di espressione:

"I soggetti dovrebbero avere un diritto sancito ex lege di ricevere una notifica concernente la sottoposizione della propria persona alla sorveglianza di comunicazioni o l'accesso ai propri dati relativi alle comunicazioni, da parte dello Stato. Riconoscendo che l'invio della notifica potrebbe compromettere l'efficacia della sorveglianza, gli individui dovrebbero comunque ricevere la notifica una volta conclusa la sorveglianza ed avere la possibilità di chiedere, successivamente, un risarcimento per l'uso di suddette misure di sorveglianza." [52]

Inoltre, il disegno di legge ugualmente non richiede un avviso ai fornitori di servizi e ai produttori di software e hardware sul metodo e la portata dell'hacking che coinvolge il loro software e/o hardware.

[52] Report del Relatore Speciale sulla promozione e protezione del diritto alla libertà di opinione ed espressione, U.N. Doc. A/HRC/23/40, par. 82, 17 Aprile 2017

10. Risarcimento e altri rimedi

Il disegno di legge non stabilisce alcun rimedio specifico o mezzo di risarcimento per gli individui danneggiati dall'illecita violazione dei propri dispositivi.

Come ha rilevato l'Alto Commissario delle Nazioni Unite per i diritti umani, i rimedi efficaci riguardano:

"Una rapida, approfondita ed imparziale indagine sulle presunte violazioni…al fine di rendere efficaci i rimedi, questi devono essere in grado di porre fine alle violazioni attualmente in corso, ad esempio, attraverso un ordine di cancellazione dei dati od altre modalità di riparazione. Gli organi incaricati di porre rimedio alle violazioni devono avere l'accesso completo e senza restrizioni a tutte le informazioni rilevanti, le risorse e le competenze necessarie per condurre le indagini, e la possibilità di emettere ordini vincolanti. Infine, ove le violazioni dei diritti umani siano più gravi, i rimedi stragiudiziali non saranno sufficienti, e sarà richiesto un procedimento penale." [53]

[53] U.N. Doc. A/HRC/27/37, supra nt. 49, par. 41