ladifesa del popolo

#06 - DATI PERSONALI

17 APRILE 2022

Cyber insicurezza

Privacy da tutelare nell'era degli attacchi informatici

mappe

LE NOSTRE IMPRONTE "DIGITALI"

I dati sono il nuovo petrolio

Miliardi di informazioni personali gestite da poche, ma potentissime lobby. E cosa succede quando finiscono in mani criminali?

Giovanni Sgobba

«**Governi del mondo, stanchi giganti di carne e di acciaio**, io vengo dal cyberspazio, la nuova dimora della mente. A nome del futuro, chiedo a voi, esseri del passato, di lasciarci soli. Non siete graditi fra noi. Non avete alcuna sovranità sui luoghi dove ci incontriamo». Con questo appello, il poeta e attivista statunitense John Perry Barlow, presentava nel 1996 la Dichiarazione di indipendenza del cyberspazio, scritta in risposta alla "Telecommunications act" americana: un manifesto che rivendicava la libertà di internet fuori dai confini di qualsiasi Paese e su cui non dovevano essere applicate leggi da parte di nessun governo. Dieci anni dopo, nel 2006, il matematico britannico Clive Humby affermava che «i dati sono il nuovo petrolio» e, senza rendercene troppo conto, società e Nazioni sono piombate nella quarta rivoluzione industriale. Web incluso.

Il corpo umano è formato al 70 per cento da acqua, ma al 100 per cento di informazioni e dati. Ogni azione inconscia o consapevole che compiamo è un dato. Il numero di battiti al minuto produce un dato. Le nostre abitudini alimentari o gusti musicali sono dati. A che ora ci svegliamo o andiamo a dormire sono dati. I nostri like su Facebook? Dati anche quelli. Una piramidale crescita, un tesoro in mano a pochissime mani al punto che Shoshana Zuboff, docente di amministrazione aziendale all'università di Harvard, parla di «colpo di stato cognitivo» perpetrato da una ristretta, ma potentissima lobby che ha il suo quartier generale nella Silicon valley californiana. Forti delle loro capacità di sorveglianza e spinti dalla necessità di accumulare profitti, i nuovi imperi privati hanno architettato un rovesciamento del potere basato su una concentrazione senza precedenti di informazioni sul nostro conto e sul potere incontrollato che ne deriva: «La tragedia dell'11 settembre 2001 ha trasformato il dibattito, spostando l'attenzione dalla necessità di approvare leggi in difesa della privacy alla raccolta totale delle informazioni. Nel 2013, il direttore della sezione tecnologica della Cia spiegava che la missione del suo ufficio era "raccogliere tutto e conservarlo per sempre" e riconosceva il ruolo delle grandi aziende del web – tra cui Google, Facebook, YouTube e Twitter oltre alle compagnie telefoniche – nel renderla possibile».

A *governance*, privacy e democrazia mai come oggi si richiede riposte decise per superare "l'insicurezza" informatica, ora che la digitalizzazione ha ingigantito la gestione economica e sociale scoperchiando falle e dimostrandoci vulnerabili ad attacchi hacker. Su tutti livelli, dai cittadini alle aziende che in qualche maniera "maneggiano" dati personali più o meno sensibili. La domanda da porsi, però, non è cosa succederebbe ai nostri dati dopo un attacco informatico, ma "e se fosse già successo e noi non ne siamo a conoscenza?" «Esistono due tipi di aziende: quelle che hanno subito attacchi e quelle che non lo sanno – spiega **Mauro Conti**, professore ordinario di cybersecurity e presidente del corso di laurea magistrale in cybersecurity dell'Università di Padova – Il dato e l'informazione esistono ancor prima dell'informatica, quest'ultima ha digitalizzato e automatizzato la fruizione. In crittografia è ancora studiato "il cifrario di Cesare", uno dei più antichi algoritmi crittografici perché da sempre si è avvertita la necessità di proteggere segreti o tenere in via confidenziale alcune cose. Oggi ci ritroviamo con banche dati enormi e in maniera più o meno cosciente dei rischi, diamo permesso all'utilizzo dei dati personali, eppure la maggior parte degli utenti non è consapevole a cosa sta acconsentendo. Pretendiamo che app e strumenti siano quotidianamente a disposizione nostra, ma sottostimiamo i rischi».

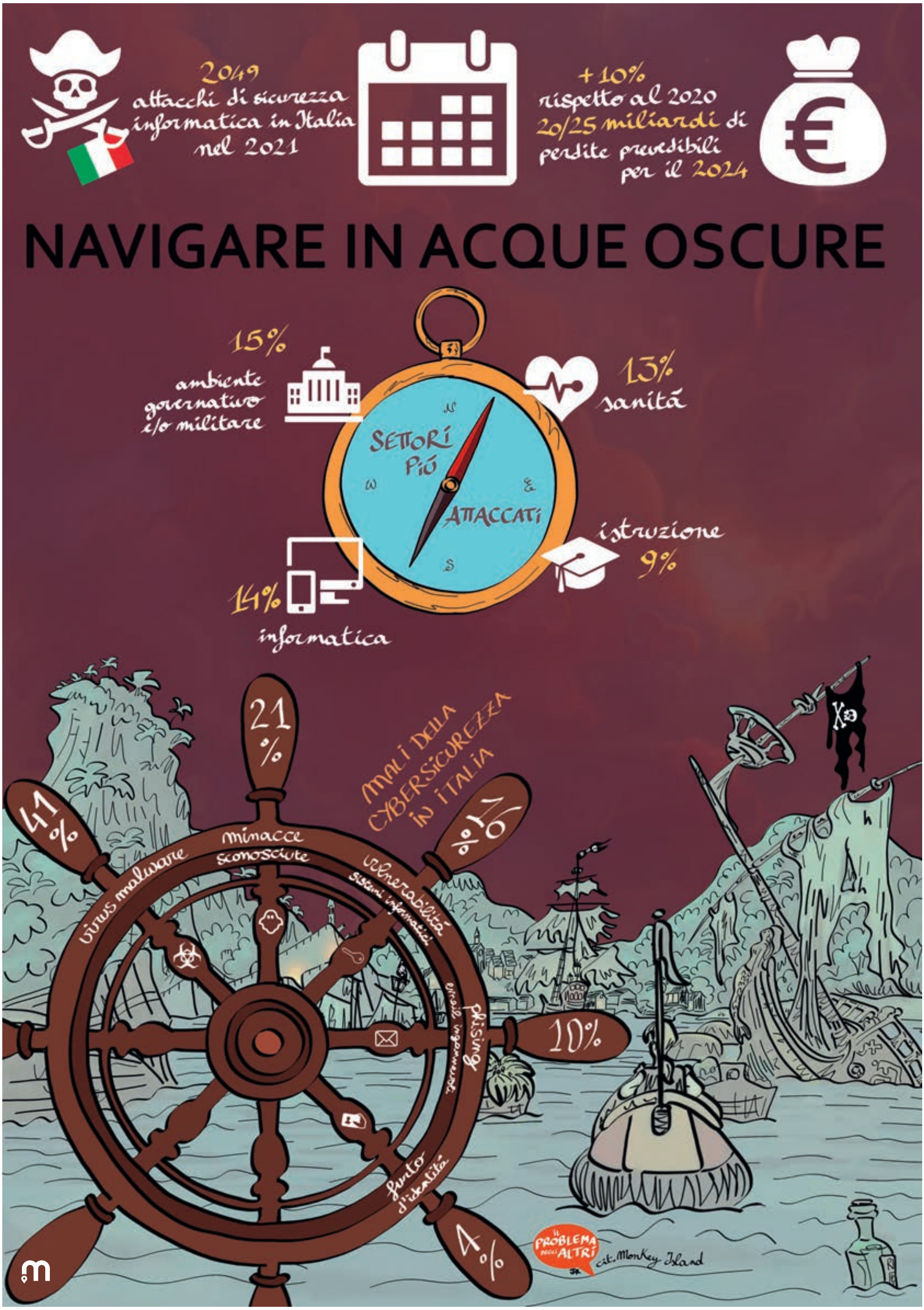
Così non ci accorgiamo che per rendere "smart" la nostra casa, finiamo con l'essere costantemente tracciati. Soprattutto dalle tv, come dimostrato dalla Northeastern University di Boston: tra gli "elettrodomestici intelligenti", i televisori smart sono quelli che più di tutti contattano servizi di profilazione, pubblicità, *tracking* e destinazioni non richieste. Eccolo il nuovo petrolio. E se magari è legato alle nostre cartelle cliniche, il dato è ancora più appetibile e prezioso. La guerra non si combatte via acqua, cielo o, come durante gli anni della cortina di ferro, nello spazio, *la cyberwar* con il collettivo di Anonymous è parte attiva del conflitto in Ucraina. «Gli strumenti diventano sempre più alla portata di chi vuole fare attacchi pur non avendo conoscenze – è il monito di Mauro Conti – Prendiamo i *ransomware*, i virus dietro ai quali si celano ricatti economici: esistono piattaforme che forniscono "servizi", tipo Amazon, con password e codici recuperati nel *dark web* e messi a disposizione di criminali e malintenzionati».

Dallo scorso settembre in Italia è attiva l'Agenzia per la cybersicurezza nazionale e per essere più sereni (si scherza) sappiate che la Nazionale italiana di hacker etici ha conquistato il terzo posto ai Campionati europei di cybersicurezza.

FOCUS IMMAGINI
"Internet delle cose" descrive la connessione degli oggetti tra di loro tramite rete. A destra, l'infografica di Giorgio Romagnoni.

2.049 sono gli attacchi informatici subiti dall'Italia nel 2021, più 10 per cento sul 2020

L'INFOGRAFICA



LO SCENARIO

Dalla guerra ai ricatti, passando per le minacce informatiche via e-mail. Parafrasando Shakespeare, siamo fatti della stessa sostanza... dei nostri dati

Proteggerci: non basta l'antivirus

Gianluca Salmaso

L'attacco che la Russia sta conducendo sul campo all'Ucraina non si combatte solo sul campo, con l'esercito, ma si sta combattendo da anni su internet, con armate di hacker, *bot* e *troll*. Se è vero che non tutti gli hacker sono russi e non tutti gli attacchi sono direttamente orchestrati dal Cremlino, va però riconosciuto alla Russia di aver raggiunto autentici successi in quella che ha assunto tutte le sembianze di una guerra asimmetrica.

Se qualche giorno fa ha fatto notizia la mossa con cui l'Fbi prima e Microsoft poi sono riusciti a bloccare attacchi provenienti da hacker russi all'Ucraina e all'Occidente, così non è successo solo pochi mesi fa quando Kiev fu messa in scacco senza troppe difficoltà. Nel primo trimestre del 2022, infatti, i siti dell'amministrazione ucraina sono stati più volte bersaglio di attacchi volti a limitarne la funzionalità, a cancellarne o a rubare i dati personali degli utenti in possesso degli enti previdenziali, assicurativi e sanitari.

«La Russia, anche prima dell'invasione dell'Ucraina – spiega **Adolfo Urso**, senatore e presidente del Copasir, il Comitato parlamentare per la sicurezza della Repubblica – si era contraddistinta per una postura aggressiva sullo scenario internazionale, caratterizzata da una implementazione del proprio impegno militare, anche in Africa e nel cosiddetto Mediterraneo allargato, e nel perseguimento di una sempre maggiore politica di potenza energetica. Sicuramente, le vicende di queste settimane comportano la necessità di un'attenzione anche maggiore, ma offrono la possibilità di una ulteriore integrazione tra i sistemi di *intelligence* europei e occidentali, anche in ordine agli investimenti sulla difesa comune europea, che non va solamente letta da un punto di vista militare, ma anche nella prospettiva di un ambito più vasto, che comprenda le diverse voci nelle quali si articola il concetto stesso di sicurezza nazionale».

Wargames, dal film ai rischi reali

Anno 1983, un giovanissimo Matthew Broderick veste i panni di un adolescente tanto svogliato a scuola quanto appassionato di computer, tanto da usare pionieristici sistemi informatici per falsificare i voti della pagella. Il protagonista poi tenta di *hackerare* i sistemi di un'azienda produttrice di videogiochi. Purtroppo per lui all'altro capo del filo non c'è la ditta ma il supercomputer che coordina la sicurezza nazionale. Calcolatori vecchia maniera, un giovane hacker e la sempre incombente guerra fredda: cosa potrebbe andare storto?

NON HANNO CEDUTO AI MALVIVENTI

Sanità sotto mira: dalla Regione Lazio all'Ulss 6 Euganea

Giovanni Sgobba

«L'attacco è partito dalla violazione di un'utenza di un dipendente in smartworking e ha colpito in un momento particolare, quando il livello di attenzione si abbassa». Un'affermazione che ha scoperto le carte, mettendo a nudo tutta vulnerabilità, anche ingenua, nostra e dei nostri sistemi. Le parole sono di Alessio D'Amato, assessore alla Salute laziale, i primi giorni dell'agosto 2021 dopo che i sistemi informatici della Regione Lazio erano stati colpiti da un *ransomware*, cioè da un attacco informatico che mira a bloccare i dati e i sistemi della vittima con l'obiettivo di ottenere un riscatto (*ransom*, in inglese). Campagna vaccinale bloccata, perdita di dati estremamente sensibili e attacco al sistema sanitario, che in tempo di Covid-19 e pandemia è il settore più esposto dopo gli ambiti governativi e militari.

Sanità sotto mira. Il caso Ulss 6. Un *dejà vu* che il Veneto ha imparato a conoscere qualche mese dopo, a dicembre, quando questa volta a essere vittima di pirati informatici è stata l'Ulss 6 Euganea.

Un conto alla rovescia, un messaggio minatorio e ricattatorio il cui senso era pagare la somma richiesta per non rendere noti tutti i dati in possesso. Firmato "virtualmente" da un gruppo di hacker internazionali collegati alla Lockbit 2.0, una *cybergang* il cui nome deriva dal virus utilizzato come grimaldello per scardinare le difese digitali. Il countdown aveva come "ora zero" prefissata il 18 gennaio scorso, ma, in assenza di risposte dell'azienda sociosanitaria che non ha ceduto al ricatto, i malviventi hanno vuotato il sacco pubblicando anticipatamente tutte le informazioni in loro possesso. Dati, ovviamente, sensibili. Nel comunicato stampa diramato successivamente dall'Ulss 6 (uno dei sette ancora consultabili a cui però non sono seguiti altri aggiornamenti sul caso) si parlava di 9.346 file con dati personali e sanitari della struttura di Schiavonia. Tamponi molecolari,

95%
della Pa non protegge i dati in sicurezza

10
milioni di italiani hanno subito violazioni web

50%
attacchi via *ransomware* con riscatto

Nulla è gratis se "paghiamo" con i nostri dati

La società Cambridge Analytica aveva sviluppato un sistema di "*microtargeting* comportamentale" cioè un tipo di pubblicità altamente personalizzata su ogni singola persona. Per fare questo sono stati utilizzati milioni di dati raccolti via Facebook. Successivamente nel 2018 ne è derivato uno scandalo che portò alla luce l'uso distorto che si può fare dei nostri dati, arrivando al punto di influenzare le elezioni americane o il referendum per la Brexit.

La sicurezza nazionale non è minacciata solo dai sabotaggi orditi dal Cremlino ma anche, come insegna il caso dell'attacco subito dall'Ulss 6 Euganea alla fine del 2021 – che ne ha paralizzato i sistemi informatici per giorni oltre al furto di migliaia di cartelle cliniche – anche dalle azioni di autentici pirati informatici che agiscono "in proprio", con l'intento di ottenere il pagamento di un riscatto per ripristinare l'efficienza dei sistemi attaccati.

«Il Comitato ha rilevato in audizione che il 95 per cento della pubblica amministrazione italiana non è ancora in condizione di proteggere adeguatamente i propri dati, come è emerso in modo eclatante in alcuni casi di attacco informatico come quello subito dalla Regione Lazio o quelli subiti da ospedali, Asl e alcune aziende strategiche – continua il presidente Urso – E il caso richiamato delle Ulss venete si inquadra esattamente in questa fattispecie. La realizzazione di un polo strategico nazionale destinato a ospitare dati e servizi digitali strategici del Paese, unitamente al presidio rappresentato dalla neocostituita Agenzia per la cybersicurezza nazionale, rappresentano elementi indispensabili affinché il necessario processo di digitalizzazione del Paese si svolga con la massima tutela della sicurezza nazionale».

Istituita nell'agosto 2021 dal Governo Draghi, l'Agenzia dovrebbe nel tempo assumere un ruolo centrale tanto nell'elaborazione quanto nella verifica delle politiche nazionali di sicurezza informatica. Il condizionale è quasi d'obbligo perché, contattata via posta elettronica, non ha mai dato riscontro.

La minaccia da contrastare è peraltro insidiosa proprio quando di mezzo c'è la posta elettronica: se collettivi di hacker come Anonymous hanno impiegato metodi raffinati per attaccare la Russia in risposta a quanto avvenuto in Ucraina, per i privati cittadini spesso i rischi maggiori arrivano dalla propria casella mail. Una comunicazione apparentemente proveniente dalla banca o una semplice richiesta di verificare i propri contatti può compromettere la sicurezza tanto dell'account quanto del dispositivo.

«L'hackeraggio dei dati può avvenire in contesti diversi, e da diversi attori – riflette Adolfo Urso – Le minacce possono essere di natura criminale, terroristica e addirittura statuale. Il tema del singolo individuo che, per cause diverse, decida di recare un attacco al sistema e alla rete è tuttavia sempre possibile. Emerge quindi con chiarezza che occorre avvalersi di una pluralità di strumenti, che esigono un costante adattamento e aggiornamento per reagire ad attacchi spesso realizzati con modalità e tempistiche imprevedibili. La prevenzione, la repressione e la cooperazione sono le aree in cui occorre agire con interventi efficaci, lungimiranti e integrati».

Spesso la prima forma di prevenzione attiene all'educazione dell'operatore – insegnare l'importanza di non aprire messaggi di dubbia provenienza, per cominciare, o connettersi solo a reti sicure – a cui però dev'essere affiancato un software in grado di compensare le minacce "invisibili" che si nascondono soprattutto su internet.

Talvolta però è proprio da questi software o dai siti a cui affidiamo la tutela delle nostre informazioni personali che scaturisce la minaccia: anche per l'interessamento del Copasir è stato recentemente bandito dalla pubblica amministrazione l'antivirus di origine russa Kaspersky, perché accusato di veicolare potenziali criticità per la sicurezza nazionale.

La facilità con cui abbiamo imparato a usare piattaforme di messaggistica istantanea o i social network tende a farci dimenticare la mole di dati, sensibili e non, che condividiamo in essi: gusti alimentari, preferenze sessuali, orientamento politico e culturale... tutto viene tracciato, salvato, messo a disposizione per campagne pubblicitarie, aumentando lo squilibrio tra ciò che sappiamo e ciò che le piattaforme sanno di noi.

Lo scandalo della società Cambridge Analytica nel 2018 portò alla luce l'uso distorto che si può fare dei nostri dati, arrivando al punto di influenzare le elezioni americane o il referendum per la Brexit. Senza dimenticare poi quanto avvenuto in Cina dove i sistemi di riconoscimento facciale furono usati già nel 2018 per tracciare gli spostamenti della minoranza musulmana degli uiguri.

I dati rappresentano però anche una vera moneta di scambio: quando il presidente americano Joe Biden promise alla presidente della commissione europea Ursula von der Leyen l'aumento delle forniture di gas per sopperire in parte alla crisi con la Russia, in cambio si fece garantire una maggiore possibilità di attingere ai dati degli europei.

L'apertura «consentirà alla Commissione di autorizzare di nuovo il flusso transatlantico di dati personali che aiuterà a mobilizzare 7.100 miliardi di dollari nelle relazioni degli Usa con l'Ue» dichiarò il presidente americano a margine di un accordo che superava in un colpo solo lustri di incomprensioni.

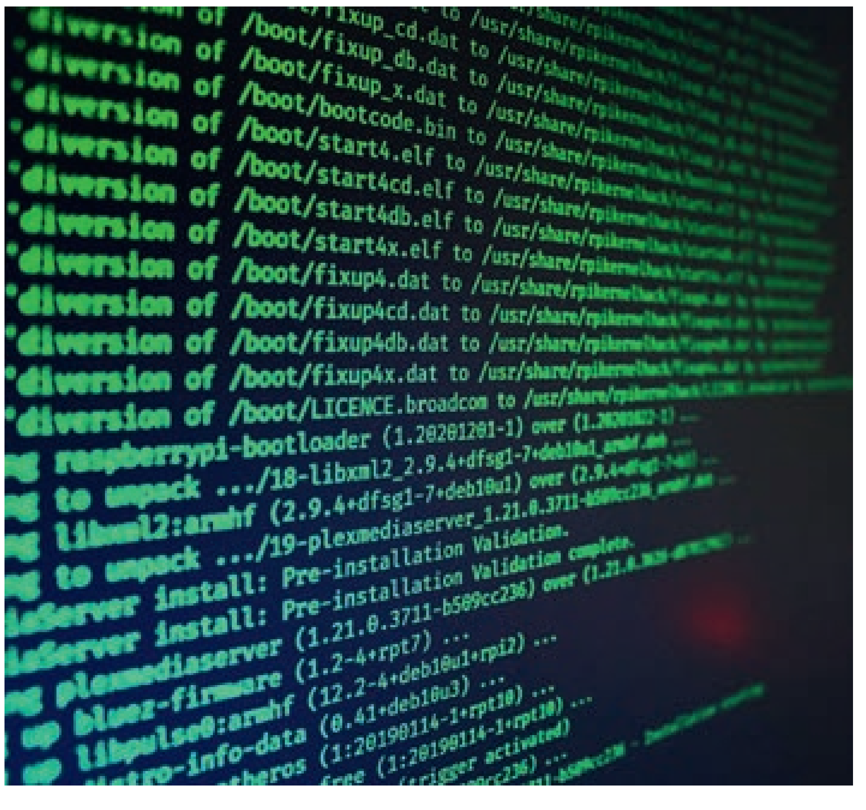

Wargames - Locandina del film del 1983.

Una "nuvola" a livello nazionale

Dove vanno a finire i dati che archiviamo su internet? I servizi cloud ("nuvola" in inglese) fanno riferimento a dei server, magazzini in cui vengono riposti e, si spera, protetti i dati ma che spesso non si trovano in Italia o in Europa. «Risulterà centrale per l'architettura di difesa il cloud nazionale a protezione dei dati della pubblica amministrazione, anche di livello locale» scriveva nella sua relazione il Copasir.

informazioni sugli stipendi e i turni del personale, referti medici ed elenchi di esami, associati ai pazienti interessati con tanto di nome, cognome, data di nascita e così via. «L'azienda e i cittadini sono vittime di un crimine vile e imperdonabile – ammoniva quattro mesi fa Paolo Fortuna, direttore generale dell'azienda sociosanitaria – Sono dati comunque difficili da raggiungere dal comune cittadino e sono frutto di attività illegale, quindi anche la semplice consultazione costituisce un reato. Quest'azienda è rimasta in possesso dei dati al 100 per cento e con prudenza e tempestività ha ripristinato la struttura e riprogrammato i servizi senza interromperli».

L'Ulss 6 non ha mai intavolato una negoziazione con i malviventi, ma l'hackeraggio ha avuto un costo . E questo supera il milione di euro. Per ricorrere ai ripari e tappare buchi digitali, l'azienda intrapreso una serie di investimenti per ripristinare il sistema, acquistare nuovi strumenti aggiornati e al passo con i tempi e per affidarsi a esperti esterni per il servizio di consulenza per la sicurezza informatica, la società Yarix di Montebelluna. E non da ultimo l'azienda ha varato un regolamento interno per disciplinare l'utilizzo consapevole degli strumenti informatici vietando l'accesso a siti e social non pertinenti a finalità professionali e lavorative.



341 per cento di ricatti in più. Ma non tutti, davanti alla minaccia, rimangono impassibili e con la schiena dritta. Chainanalysis, una società di analisi di criptovalute con diverse sedi sparse nel mondo, ha calcolato che tra il 2019 e il 2020 a livello globale il numero di riscatti pagati a seguito di attacchi *ransomware* è aumentato del 341 per cento, passando da 93,4 milioni di dollari a 412 milioni. E nessuno è al momento immune: a inizio aprile sotto scatto è finito il ministero per la Transizione ecologica, ma la lista si allunga e comprende Trenitalia, piccole amministrazioni comunali e, pare, anche la Banca d'Italia.

DALLA SERIE TV ALLA GUERRA

Anonymous, web-attivisti schierati a colpi di "click"

COLPI IN RETE

Ernesto Milanesi

Nella cifra binaria del sistema informatico si annida anche l'alternativa. Una serie tv "sovversiva", l'informazione svincolata dai media, la "legione" che libera i dati del potere. È l'uso diverso dell'intelligenza artificiale: protagonismo che abbatte recinti e attivismo in nome dei diritti, con il pc come leva di conflitto con altri mezzi.

"Mr Robot", la ribellione. Il produttore e regista Sam Esmail ha sceneggiato per Usa Network 45 episodi in quattro stagioni: il futuro premio Oscar Rami Malek veste i panni di Elliot Alderson, ingegnere al servizio della sicurezza informatica. Al lavoro per il colosso che monopolizza vite e coscienze alterna la vocazione da hacker che scardina ipocrisia e dominio. Dati nebulizzati, privacy sotto controllo, consumo di profitti. Uno scenario realistico, con il protagonista che confessa: «Non ho mai trovato difficile hackerare la maggior parte delle persone. Se li ascolti, li guardi, le loro vulnerabilità sono come un'insegna al neon avvitata nella loro testa». È il metodo con cui si può perfino scardinare la piramide inossidabile.

Indymedia, sito *no global*. Entra nel web il 24 novembre 1999 e rivoluziona il flusso dell'informazione. Con *seattle.indymedia.org* l'indipendenza mediatica si sposa immediatamente con i movimenti *no global*. Indymedia si è imposto come il primo, identitario e radicato "social network". Una specie di evoluzione del fenomeno delle radio libere anni Settanta: decine di "nodi" in grado di documentare con foto, video, audio le "notizie" altrimenti escluse dalle pagine di carta e dai notiziari tv. Genova 2001, quando i diritti costituzionali sono stati sospesi, il media center alternativo al G8 era stato allestito proprio con i criteri di Indymedia: libero accesso per tutti. Ed è stata la migliore fonte di informazione per documentare tutto nel dettaglio: piazza Alimonda, la scuola Diaz, il lager di Bolzaneto.

Anonymous "in trincea". Ha pubblicato i files della banca centrale russa, i piani di invasione dell'Ucraina, l'identità di 120 mila soldati di Putin, il profilo di Omurbekov Azatybek Asanbekovich, il comandante dell'unità 51460, 64esima brigata di fucilieri motorizzati, accusato del massacro di Bucha. Anonymous resta "in trincea" a modo suo, dopo aver mobilitato hacker e violato archivi di dati ultra-sensibili. È perfino entrato nel circuito della videosorveglianza del Cremlino. Ha sposato l'Ucraina, perché il collettivo cibernetico senza nome lotta da sempre contro le ingiustizie. Nato nel 2003, Anonymous mutua il nome assegnato ai visitatori senza identità dell'*imageboard* in inglese "4chan" che si concentrava su anime e manga. Il simbolo scelto è la maschera di Guy Fawkes, cospiratore cattolico inglese che tentò di uccidere il re protestante Giacomo I nel 1605, divenuta famosa con il film *V per vendetta*. Nell'arco di vent'anni, Anonymous ha messo a segno decine di clamorose "intrusioni". E in Italia ha attaccato fra gli altri Enel, Agcom, Trenitalia, Viminale e Expo 2015.

Due miliardi di computer nel mondo

I nostri pc sono i "nipoti" di Eniac, primo calcolatore elettronico costruito nel 1946 da John Mauchly e John Eckert: 18 mila valvole, pesava 30 tonnellate e occupava 140 metri quadrati. Oggi nel pianeta funzionano due miliardi di computer, mentre l'anno scorso ne sono stati venduti 341 milioni con Lenovo al top davanti a Hp, Dell e Apple. E il 2021 ha fatto registrare il più alto volume di distribuzioni di pc dal 2013.

Se il sistema si arresta... Edward Snowden, Julian Assange e Chelsea Manning lo hanno dimostrato: il sistema operativo del potere si può sempre arrestare. E i "Panama papers", con oltre 11 milioni di documenti confidenziali, hanno denudato 214 mila società offshore che facevano capo allo studio di Mossack Fonseca. Come sottolineava il giornalista del *Manifesto* **Benedetto Vecchi** «in una situazione dove la rete è diventata medium universale, Assange ha intuito il potenziale controinformativo. Con un lavoro meticoloso di verifica delle informazioni, ha messo online documenti mai smentiti, senza mai mettere in pericolo la vita di nessuno». Eppure è rinchiuso a Belmarsh dall'11 aprile 2019 e rischia l'estradizione negli Usa.

Un monito d'attualità. Lo ha lanciato ancora nel 2016 **Geert Lovink**, teorico dei media e direttore dell'Institute of network cultures di Amsterdam: «Forse i computer sono macchine cristiane. Umberto Eco aveva ragione a proporre la distinzione tra Mac come computer cattolico e Microsoft come interfaccia protestante. Ma tutt'e due sono sistemi operativi cristiani. Le reti collegano, creano una comunità. Enfatizziamolo in questi tempi disperatamente nichilisti».

I dati, il nuovo “petrolio” che ingolosisce le criminalità

I muli del denaro - Persone ignare usate per riciclare soldi sporchi.

WEB-FRODI

Rossana Certini

Durante il biennio della pandemia in Italia si è verificato un *boom* di delitti informatici. A metterlo nero su bianco è l’associazione Libera che, nel report *La tempesta perfetta*, calcola un aumento del più 38 per cento dei crimini informatici. Dall’analisi dei dati emerge che il primato spetta alla Lombardia (più 86 per cento) seguita da Basilicata (più 83 per cento) e Puglia (più 81 per cento).

La polizia postale calcola che nel 2021 il settore del *financial cybercrime* ha registrato 174 attacchi informatici ai sistemi finanziari di grandi e medie imprese, per un ammontare complessivo di oltre 61 milioni di euro sottratti attraverso frodi telematiche, 32 milioni dei quali recuperati dall’azione tempestiva degli investigatori. Ma l’Italia non è sola in questa crescita. L’ultimo rapporto Clusit (associazione italiana per la sicurezza informatica) stima che nel 2021 nel mondo c’è stato un aumento del 10 per cento degli attacchi informatici che crescono sia in quantità che in qualità. Il report analizza 2.049 cyber-attacchi noti (individuati e classificati nell’anno a livello globale, Italia inclusa) e li confronta con quelli del triennio precedente. L’associazione in undici anni di attività ha identificato, classificato e valutato oltre 14 mila attacchi informatici gravi (in media 1.274 all’anno, più di 100 al mese). Di questi 7.144 si sono verificati negli ultimi quattro anni, dimostrando un’accelerazione impressionante nella frequenza delle minacce cibernetiche.

¶

«Questa crescita – spiega **Pierluigi Paganini**, esperto di cybersecurity e intelligence, fondatore di Cybhorus – è diretta conseguenza dell’aumento della componente tecnologica nella nostra società. Sappiamo bene che usufruiamo, più o meno consapevolmente, di molti servizi in rete che ci richiedono l’inserimento di dati che possono essere oggetto di attacchi cybernetici. Distinguiamo, però, crimini che hanno obiettivi finanziari e attacchi, messi a punto da attori che operano per conto di governi, come la Russia, la Cina e l’Iran, che hanno finalità di spionaggio e sabotaggio industriale o diplomatico. È interessante notare, anche, come soprattutto le Nazioni che sono sotto embargo, per esempio la Corea del Nord, in questi anni si sono specializzate in attacchi finanziari con l’intento di raccogliere fondi per operazioni militari».

Dai dati Clusit emerge che gli attacchi cybernetici si sono verificati nel 45 per cento dei casi nel continente americano (in leggero calo rispetto al 2020). Sono invece cresciuti gli attacchi verso l’Europa, che superano un quinto del totale (21 per cento, contro il 16 per cento dell’anno precedente) e verso l’Asia (12 per cento, rispetto al 10 per cento del 2020). Resta sostanzialmente invariata la situazione degli attacchi verso Oceania (due per cento) e Africa (un per cento).

L’emotività pandemica come esca

A ottobre 2021 è stato pubblicato il nono report di Enisa, l’agenzia europea della cybersecurity. Tra i vari aspetti analizzati, lo studio si è soffermato sulla vulnerabilità dei singoli individui. L’ingegneria sociale (lo studio del comportamento di una persona al fine di carpire informazioni utili) resta una delle tecniche più utilizzate per far leva sull’emotività degli utenti e indurli in trappole pericolose. Il Covid-19, infatti, ha fornito un pretesto per adescare persone in cerca di notizie su pandemia, cure e vaccinazioni. Molti criminali si sono finti figure mediche competenti o hanno attaccato i lavoratori in smart working.

¶

In aumento anche il fenomeno dei *money mules* (letteralmente “muli del denaro”) una modalità sempre più consolidata per realizzare frodi online. Per riciclare il denaro sporco e proventi tramite financial cybercrime, la criminalità organizzata si serve di persone che sono reclutate con vari espedienti, spesso ignare dell’illegalità delle pratiche stesse. La diffusione di questa modalità ha spinto l’Europol a dedicare al contrasto del fenomeno una specifica azione ad alto impatto: a fine novembre 2021 la polizia postale e le forze di polizia cyber di altre 27 Nazioni coordinate da Europol e Interpol hanno portato a termine la settima edizione dell’operazione Emma. Grazie al supporto di oltre 400 istituti bancari e altre istituzioni finanziarie, sono state individuate settemila transazioni bancarie fraudolente, sono state avviate oltre 2.500 indagini autonome, riuscendo a prevenire frodi per un danno stimato in 67,5 milioni di euro. Individuati più di 18 mila “muli” coordinati da 324 organizzatori.

NON SOLO SCAMBI ILLECITI

La “rete oscura” unica risorsa contro le dittature

Nel 2021 l’Italia è stata il Paese leader in Europa nel contrasto al *carding* nel *dark web*, che consiste nella compravendita di codici di carte di credito/debito compromesse. La polizia postale al termine di una lunga attività di monitoraggio, prevenzione e repressione, durata circa tre mesi, ha recuperato 16 milioni di euro e il blocco di 49.761 codici di carte di credito trafugate. Un risultato possibile attraverso l’analisi puntuale delle tracce informatiche che hanno consentito di approfondire il fenomeno del *carding* sul ***dark web***.

Ma come definire il dark web? È la parte oscura del ***world wide web*** (il più comune *www* che digitiamo per accedere a un sito) e sottogruppo del ***deep web*** che è l’insieme dei contenuti presenti su internet e non indicizzati dai comuni motori di ricerca come Google. Uno spazio accessibile mediante l’uso di apposite applicazioni software. Ogni cosa ha un valore sul mercato del *dark web* dalle credenziali ai contenuti delle mail, agli accessi a infrastrutture aziendali. Tutto viene venduto e acquistato in tempi brevissimi dai criminali del web. «Non dobbiamo però demonizzare il *deep web* – precisa **Andrea Pin**, professore associato del dipartimento di Diritto pubblico, internazionale e comunitario dell’Università di Padova – perché è spesso l’unico spazio di libertà di espressione che hanno le persone che vivono in regimi dittatoriali dove i soggetti che vogliono esprimere il dissenso possono farlo solo in una dimensione che non è sorvegliata da chi detiene il potere». *(R. C.)*

PROTEZIONE PERSONALE

Sicurezza e... biscotti

I cookies agevolano il nostro navigare online, ma veicolano preziose informazioni. Come deve comportarsi l'utente?

TUTELARSI

Rossana Certini

La protezione dei dati personali è un diritto fondamentale dell'individuo che oggi è tutelato, in particolare, dal regolamento 2016/679 del Parlamento europeo e del Consiglio e che disciplina il trattamento dei dati personali indipendentemente dal fatto che questo sia effettuato o meno nell'Unione europea. Ma tutto questo non basta a metterci al riparo dalle conseguenze dei crimini informatici perché il vero oro nero moderno non è tanto il dato in sé ma l'uso statistico che attraverso l'insieme dei dati personali raccolti si riesce a estrapolare.

Infatti, come spiega **Andrea Pin**, coordinatore del corso di laurea triennale in Diritto e tecnologia all'Università di Padova «lo sviluppo dell'informatica e dell'analisi dei dati permette, incrociando studi psicologici e sociologici, di raccogliere e processare informazioni e persino conoscere aspetti molto intimi dei soggetti e con questi dati predire le azioni di singoli e gruppi. L'intelligenza artificiale è, dunque, in grado di compilare la biografia, le preferenze personali e gli stili di vita degli utenti che in vari momenti si connettono alla rete. Questi dati possono essere evidentemente utilizzati nel migliore dei casi per ragioni commerciali o fini informativi».

Da queste prime riflessioni si deduce quanto importate sia stata l'approvazione, lo scorso giugno, da parte del Garante per la protezione dei dati personali delle nuove linee guida in materia di consenso da parte dell'utente attraverso i *cookies* ("biscotti" in inglese) che sono quei piccoli file di testo che i siti visitati dagli utenti inviano ai dispositivi usati per la consultazione per essere memorizzati e poi ritrasmessi agli stessi siti in occasione della visita successiva. Infatti, i *cookies* se da un lato velocizzano gli accessi ai siti web da parte degli utenti e semplificano la fruizione di alcuni servizi internet, dall'altro sono molto utili per i soggetti che gestiscono i siti stessi perché consentono la raccolta e il trattamento di vari dati personali. Informazioni che possono essere utilizzate a fini di marketing, di profilazione e di condivisione con terze parti.

¶

Altro discorso è quello del furto dei dati personali per fini estorsivi per mezzo di attacchi informatici: «Spesso si pensa che alle spalle ci siano dei gruppi criminali esperti e strutturati o addirittura orchestrati da potenze straniere – rivela **Giancarlo Di Lieto**, capo della sicurezza di Innovery, azienda italiana specializzata in cyber security – In verità questi sono solo una minima parte degli attacchi di cui sentiamo parlare ogni giorno, la maggior parte sono attuati da singoli individui, che sviluppano programmi informatici allo scopo di guadagnare. La tipologia più diffusa di questo genere di attacchi sono i *ransomware*, che hanno lo scopo ultimo di ottenere un riscatto. Si tratta di programmi software creati per andare a bloccare i dati della vittima, rendendoli illeggibili per il proprietario, senza tuttavia comprometterli definitivamente perché qualora finissero danneggiati l'attaccante non avrebbe alcun riscatto».

Un'indagine fatta sui clienti Fastweb nel 2021 e riportata nel report Clusit 2022 stima che c'è stato un incremento di tecniche per il furto dei dati personali degli utenti. Tra queste il *phishing* rappresenta la modalità di attacco più utilizzata, con un peso del 60 per cento sul totale. Questa è una tecnica illecita utilizzata per appropriarsi di informazioni riservate relative a una persona o a un'azienda: username e password, codici di accesso, numeri di conto corrente, dati del bancomat e della carta di credito con l'intento di compiere operazioni fraudolente. La truffa avviene di solito via e-mail, ma possono essere usati anche sms, chat e social media.

¶

«La prevenzione – prosegue Di Lieto – resta sempre la miglior difesa in questi casi. È importante effettuare backup regolari dei propri dati, ricordando di utilizzare differenti supporti da hard disk esterni fino al cloud». Come in ogni campo anche in questo purtroppo il fenomeno criminale è sempre più veloce del legislatore anche se in Europa e in Italia vigono leggi in materia di tutela dei dati personali che sono tra le più avanzate del mondo. È importante, quindi, che il singolo individuo faccia attenzione a quando utilizza i suoi dati nella rete. «Non tutti sanno – precisa **Riccardo Borsari**, professore associato di diritto penale nel dipartimento di Diritto pubblico, internazionale e comunitario dell'Università di Padova – che nel web nulla si cancella ma anche se si elimina qualcosa resta sempre una traccia da qualche parte. Quindi sarebbe bene limitare il racconto della nostra vita quotidiana sui social, nelle chat e nella rete in generale». Nei mesi estivi del 2021, per esempio, il Garante ha promosso la campagna "E-state in privacy", un *vademecum* sull'uso prudente delle tecnologie digitali in vacanza. Selfie e acquisti online, social network e geolocalizzazione sono tappeti rossi srotolati ai piedi dei criminali: nell'ingenuità di questi gesti diventa facilissimo sapere, per esempio, quando un'abitazione è vuota.

Privacy e bilanciamento delle esigenze

Secondo alcuni studi, 68 *like* su Facebook consentirebbero di identificare il colore della pelle, l'orientamento sessuale o politico di un utente, con percentuali di precisione che superano l'80 per cento.
Sul concetto di privacy e tutela dei dati personali un dibattito ha riguardato la pandemia e le app nate per tracciare l'esposizione di ciascuno a soggetti in quel momento positivi. A seguito di un confronto con il Garante per la protezione dei dati personali, la soluzione è stata individuata in una serie di tutele – tra cui la volontarietà dell'uso della app, l'anonimità dei contatti, la cancellazione dopo breve tempo dei dati raccolti – al fine di scongiurare forme di controllo di massa sugli spostamenti e le frequentazioni della popolazione. Un bilanciamento ottenuto esaminando le diverse esigenze.