

# **Spazio cibernetico bene comune**

## **Protezione dei dati, sicurezza nazionale**

CONTRIBUTI



**Atti del Convegno - 30 gennaio 2020**



**GARANTE  
PER LA PROTEZIONE  
DEI DATI PERSONALI**



GARANTE  
PER LA PROTEZIONE  
DEI DATI PERSONALI

Antonello Soro, Presidente  
Augusta Iannini, Vice Presidente  
Giovanna Bianchi Clerici, Componente  
Licia Califano, Componente

Giuseppe Busia, Segretario generale

Piazza Venezia, 11  
00187 Roma  
[www.garanteprivacy.it](http://www.garanteprivacy.it)



GARANTE  
PER LA PROTEZIONE  
DEI DATI PERSONALI

# Spazio cibernetico bene comune

Protezione dei dati, sicurezza nazionale

Atti del Convegno  
30 gennaio 2020

In questo volume sono raccolti i contributi di studiosi ed esperti intervenuti al Convegno “*Spazio cibernetico bene comune. Protezione dei dati, sicurezza nazionale*” organizzato dal Garante per la protezione dei dati personali in occasione della “Giornata europea della protezione dei dati personali” 2020.

# Indice

<b>Spazio cibernetico bene comune</b>	<b>5</b>
<b>Protezione dei dati, sicurezza nazionale</b>	
<b>Antonello Soro</b>	
<i>Presidente del Garante per la protezione dei dati personali</i>	
<b>Sicurezza cibernetica e libertà individuale: una prospettiva comune</b>	<b>19</b>
<b>Raffaele Volpi</b>	
<i>Presidente del Copasir</i>	
<b>Data commons. Privacy e cybersecurity sono diritti umani fondamentali</b>	<b>29</b>
<b>Arturo Di Corinto</b>	
<i>Giornalista esperto di cybersecurity, Autore e inviato di “Codice” - Rai 1</i>	
<b>Cybersecurity e privacy nel futuro iperconnesso</b>	<b>43</b>
<b>Stefano Zanero</b>	
<i>Professore Associato Politecnico di Milano</i>	
<b>Sicurezza informatica: i nuovi dati</b>	<b>57</b>
<b>Clusit e Osservatorio Cybersecurity &amp; Data Protection Politecnico di Milano</b>	
<b>Gabriele Faggioli</b>	
<i>Presidente del Clusit, Adjunct Professor MIP-Politecnico di Milano</i>	

# Spazio cibernetico bene comune

## Protezione dei dati, sicurezza nazionale



**Antonello Soro**

*PRESIDENTE DEL GARANTE*

*PER LA PROTEZIONE DEI DATI PERSONALI*

# Spazio cibernetico bene comune

## Protezione dei dati, sicurezza nazionale

**Antonello Soro**

*Presidente del Garante per la protezione dei dati personali*

La sicurezza della dimensione cibernetica è costantemente esposta a minacce: minacce sempre più "ibride", tali da configurare una sorta di *cyber guerriglia* permanente.

Nel 2019 il *cybercrime* è cresciuto del 17% a livello mondiale rispetto alle cifre del 2018: anno già definito, per quel che riguarda l'Italia, il peggiore per la sicurezza cibernetica.

Gli esperti hanno tracciato preoccupanti previsioni sui possibili rischi e sulle tendenze per il 2020, delineando uno scenario fatto di attacchi sempre più sofisticati.

Nei mesi scorsi, la Polizia Postale ha portato alla luce quello che parrebbe configurarsi come il più grave attacco alle banche dati istituzionali finora realizzato, con tecniche di *phishing* che consentivano l'accesso a sistemi informativi tra i più rilevanti per il Paese, dai quali estrarre dati da rivendere ad agenzie investigative e di recupero crediti.

Ma gli attacchi informatici sono divenuti anche mezzi d'ingegneria bellica. Basta pensare ai recenti avvenimenti in Medio Oriente, anticipazione di quel che sarà il paradigma dello scontro militare nei prossimi anni: droni armati e attacchi informatici utilizzati quali vere e proprie armi, dotate di una potenza straordinariamente maggiore.

Quella cibernetica è dunque la dimensione su cui si sposta sempre più la dinamica dei conflitti, palesi o latenti, tra Stati e tra soggetti, operata attraverso dati e sistemi informativi.

Ed è, peraltro, è l'unica dimensione della sicurezza e della

difesa sostanzialmente priva di un'adeguata cornice di diritto internazionale.

Un'efficace strategia di prevenzione dei rischi cibernetici presuppone quindi, anzitutto, la consapevolezza dei fattori su cui si basano, rispettivamente, azione e reazione: la tecnologia e il diritto. Se, infatti, le nuove tecnologie sono il presupposto essenziale della "potenza geometrica" delle nuove minacce, il diritto è l'unica risorsa capace di mettere la tecnica al servizio dell'uomo, della libertà, della sicurezza.

E, anzi, un'alleanza di tecnologia e diritto può rappresentare l'architrave di una risposta democratica e lungimirante alle nuove minacce del digitale, inevitabilmente connesse agli opposti, straordinari benefici.

Questo presuppone anzitutto il massimo equilibrio tra le discipline deputate a governare il rapporto tra le libertà e il lato oscuro della tecnica, ovvero quella di protezione dati e quella a tutela della sicurezza cibernetica.

Tra le quali intercorre un rapporto indubbiamente complesso, ma che tra antagonismi e inattese sinergie, dice moltissimo di una società in cui l'esibizione incontenibile della vita privata riflette una crisi profonda di fiducia e coesione sociale: elementi - questi - su cui in passato si fondava un'assai diversa percezione tanto della sicurezza quanto della libertà.

Da un lato, infatti, la tutela della sicurezza cibernetica (quinta, ma sempre più rilevante dimensione della sicurezza nazionale), ha legittimato limitazioni incisive della *privacy*, in nome del contrasto a minacce tanto immanenti quanto pulviscolari, con il ricorso a strumenti investigativi spesso di tipo massivo.

*Social e signal intelligence*, sorveglianza strategica (e non più solo "mirata"), *data mining*: sono solo alcune delle forme che può assumere l'azione di prevenzione e che estende il suo raggio di azione quanto più la società iperconnessa alimenta continui flussi informativi.

La potenza della tecnologia, da un lato, e le caratteristiche della minaccia cibernetica (acefala, mutevole, nebulosa) dall'altro, ampliano dunque, inevitabilmente, lo spettro dell'azione investigativa.

Questo ha implicazioni importanti sotto il profilo delle libertà e degli equilibri democratici.

Se pensiamo che - nel nostro Paese - i gestori conservano, ogni giorno, circa 5 miliardi di tabulati di traffico telefonico e telematico per fini di contrasto, dobbiamo chiederci anzitutto se nell'ambito di una massa così enorme di dati sia davvero possibile rinvenire quelli utili; se, insomma, estendendo così a dismisura il pagliaio sia ancora ragionevole pensare di poter trovare l'ago.

E un'azione di contrasto così penetrante determina una limitazione della *privacy* che sarà legittima solo se e in quanto strettamente conforme al principio di proporzionalità, su cui la Corte di giustizia ha costruito l'architrave del rapporto tra prevenzione e libertà.

Ma, circoscritte le politiche di sicurezza e i poteri degli organi di contrasto entro il perimetro della proporzionalità, sarà chiaro come quello tra protezione dati e *cybersecurity* non sia un gioco a somma zero ma, anzi, un rapporto fatto di sinergie e reciproche funzionalità.

L'esperienza del protocollo d'intenti con il Dis è, in questo senso, emblematica. Esso, infatti, è stato siglato proprio quando, nel 2013, è emersa l'esigenza di un parallelismo tra estensione dei poteri degli Organismi e corrispondente aggiornamento delle funzioni di garanzia dell'Autorità.

Nato, dunque, per bilanciare esigenze di sicurezza e protezione dei dati, tale strumento innovativo ha dimostrato come questi beni giuridici essenziali, tutt'altro che necessariamente antagonisti, siano invece assai più complementari di quanto si possa immaginare.

E questo perché la *cybersecurity* implica anzitutto, inevita-

bilmente, la protezione dei dati e delle infrastrutture di cui è composto l'ecosistema digitale.

E' significativo che, a seguito della direttiva NIS e del Gdpr, il protocollo sia stato integrato, prevedendo la comunicazione, da parte del Garante ai Servizi, dei *data breach* suscettibili di rilevare per la sicurezza nazionale.

Del resto, una normativa che fa della tutela dei dati e dei sistemi dal rischio informatico il suo fulcro essenziale, non può che promuovere quelle condizioni complessive di resilienza indispensabili per la sicurezza cibernetica.

La responsabilizzazione dei titolari promossa dal Regolamento, rispetto al rischio "sociale" derivante da sistemi informatici permeabili è, in questo senso, una risorsa preziosa.

Il legislatore europeo ha anzi instaurato una significativa simmetria tra protezione dati e sicurezza cibernetica, particolarmente evidente in alcuni istituti che accomunano il Regolamento, la direttiva NIS e lo stesso regolamento 2019/881 sulla *cybersecurity*.

Tale complementarietà tra protezione dati e sicurezza cibernetica non è, del resto, casuale, se si pensa alla funzione originaria della prima nell'ordinamento europeo, considerata un bene giuridico che ciascuno Stato membro avrebbe dovuto garantire per poter entrare nell'area Schengen, in quanto presupposto per la sua sicurezza.

Gli sviluppi più recenti dimostrano quanto lungimirante fosse tale concezione del rapporto tra protezione dati e sicurezza: in un'economia e una società fondata sui dati, proteggere questi significa tutelare ad un tempo i singoli e la collettività.

Protezione dati come presupposto ineludibile della sicurezza individuale e collettiva, dunque, tanto più necessario all'epoca dei *big data* e dell'Internet "di ogni cosa".

In tale contesto, in cui ciascun oggetto di uso quotidiano può rappresentare il canale d'ingresso di potenziali attacchi informatici e in cui quindi le fonti di rischio si moltiplicano a di-

smisura, è indispensabile fare della protezione dei dati, dei sistemi e delle infrastrutture l'obiettivo prioritario delle politiche pubbliche, perché da questo dipende la tutela della persona ma anche la sicurezza nazionale.

La crescente complessità dei sistemi genera, infatti, vulnerabilità sfruttate per attacchi informatici che possono paralizzare reti di servizi pubblici essenziali, canali di comunicazione istituzionali di primaria importanza, con un impatto, dunque, concretissimo sulla vita pubblica.

Le caratteristiche delle minacce, come per il terrorismo, non sono più prevedibili in quanto pulviscolari e in continua evoluzione.

La difesa diviene così asimmetrica anche perché le catene, più complesse, su cui si articolano i flussi informativi presentano una molteplicità crescente di anelli deboli.

Ciò evidenzia come le sinergie che caratterizzano il rapporto tra protezione dati e *cybersecurity* non siano soltanto normative ma attengono a un livello più profondo e strutturale, perché tendono entrambe alla protezione della realtà digitale, dei dati e i sistemi considerati non isolatamente, ma nelle loro reciproche inferenze.

La sicurezza cibernetica è stata, del resto, definita bene comune, la cui tutela avvantaggia tutti, proprio perché attiene a una realtà, quale quella digitale, fondata sull'interdipendenza di dati, sistemi, soggetti.

In tale prospettiva abbiamo orientato la nostra azione in questi anni, rilevando anzitutto l'esigenza di razionalizzare il patrimonio informativo, soprattutto pubblico, per ridurre la superficie d'attacco da cui estrarre dati spesso utilizzati a fini di spionaggio.

Abbiamo poi sottolineato le implicazioni dovute alla sempre più frequente esternalizzazione a privati di segmenti importanti dell'attività amministrativa o, ancor più, investigativa, che ne rendono alquanto più permeabile la filiera.

Ricordo, in tal senso, la significativa attività svolta nel 2014 rispetto ai nodi di interscambio internet (ixp), gestiti da privati non sempre in modo adeguato e dalla cui sicurezza dipendono, tra l'altro, la sicurezza nazionale, l'efficacia delle indagini, l'incolumità dei singoli.

Come, del resto, dimostrano i casi *Hacking Team* ed *Exodus*, la vulnerabilità dei sistemi utilizzati dai privati incaricati e la negligenza frequente nell'osservanza degli obblighi di protezione espone a un rischio insostenibile non solo la riservatezza dei cittadini, ma anche i dati investigativi e spesso persino la sicurezza nazionale.

Solo l'adozione di misure adeguate, da parte di ciascun soggetto coinvolto in ogni fase dell'attività captativa, può dunque contribuire a minimizzare i rischi connessi alla frammentazione dei centri di responsabilità, derivanti dal coinvolgimento di soggetti diversi nella "catena" delle attività investigative.

E la stretta dipendenza della sicurezza della rete da chi ne gestisca i vari snodi e "canali" pone il tema della sovranità digitale, da declinarsi non in chiave nazionalistico-autarchica, quanto piuttosto investendo, nella governance della dimensione digitale, la propria identità giuridica e politica.

E poiché le minacce sono globali, credo che l'obiettivo debba essere la complessiva assunzione di responsabilità pubblica rispetto a un interesse, quale la sicurezza cibernetica, da cui dipende in primo luogo l'indipendenza dei Paesi e che deve sempre più declinarsi in chiave sovranazionale, spostando, proprio come è stato per la protezione dati, il proprio orizzonte sulla dimensione (almeno) europea.

Di fronte a minacce che vanno dalla guerra cibernetica all'antagonismo politico digitale, dunque, le politiche pubbliche devono mettere al centro il valore della protezione dati quale condizione di competitività, sicurezza e assieme di libertà, per non soggiacere alla spinta neocolonialista delle autocrazie digitali.

Non a caso, l'Europa ha reso la protezione dati un fattore identitario, ritrovandovi, proprio in un momento in cui riaffiorano le spinte divisive, quell'aspirazione federale così ostacolata in altri campi e tale da segnare un vero e proprio divario transatlantico nella gestione del rapporto tra tecnica e diritti, economia e libertà.

E questa vocazione unitaria (ma anche, appunto, identitaria), superando i particolarismi che spesso privano il diritto del suo necessario "sguardo lungo", ha consentito a questa disciplina di divenire il fronte più avanzato di *governance* del digitale, una vera e propria costituzione per l'algoritmo, a cui poi molte altre normative (anche extraeuropee) hanno attinto.

La forza attrattiva e la vocazione "costituzionale" della protezione dati si fondano, del resto, sulla lungimiranza di alcuni suoi istituti essenziali.

Si pensi all'affermazione - pressoché unica nel panorama giuridico attuale e capace di offrire tutela in ogni campo - del diritto alla non esclusività e non discriminatorietà della decisione algoritmica, che non deve insomma divenire parametro unico né tantomeno distorsivo di valutazione della persona.

Le implicazioni di ordine giuridico-costituzionale, politico-economico, persino etico di questa previsione sono determinanti e, se forse non risolutive, certamente ineludibili in una società sempre più fondata sul potere dell'algoritmo.

Inoltre, la prevista "extraterritorialità" del Regolamento - che si applica anche a titolari extra-Ue per il fatto di trattare dati di quanti si "trovino" in Europa - ha implicazioni dirompenti sotto il profilo giuridico, economico, simbolico.

Non solo, infatti, ciò consente di attrarre nel diritto europeo i giganti del *web*, sfuggenti a ogni altro tentativo di regolazione, assicurando a chiunque si trovi in Europa (non solo ai "cittadini", come doveroso per un diritto fondamentale) un paniere di diritti non derogabile in ragione della sede, più o meno di comodo, dell'attività aziendale.

Tale previsione afferma, con tutta la forza della regola che è insieme principio, che in uno spazio defisicizzato come la rete la sovranità vada declinata in forme nuove, meno legate al tradizionale criterio di territorialità e più attente, invece, alla capacità degli Stati di rendere effettiva la tutela dei diritti e la stessa forma democratica, di fronte a sempre nuove spinte illiberali.

Sono significativi, in tal senso, i rischi cui un uso manipolativo dei dati personali, anche da parte di potenze estere, può avere sulla sovranità nazionale e sulle scelte politiche essenziali che ne determinano l'esercizio.

La vicenda *Cambridge Analytica* ha dimostrato, infatti, come il *microtargeting* basato sulla profilazione dei cittadini e la conseguente propaganda elettorale, mirata in base al tipo di elettore stilato dall'algoritmo, determini un pesante condizionamento del processo di formazione del consenso, che può essere gestito da potenze straniere per orientare a loro favore il risultato elettorale.

Non a caso, a seguito della vicenda *Cambridge Analytica*, il Congresso Usa ha iniziato a discutere un disegno di legge federale per la protezione dati modellato sul paradigma europeo e la California ha approvato una normativa in tal senso.

È infatti apparso evidente come il contrasto dello sfruttamento dei dati personali in funzione distorsiva del consenso elettorale sia funzionale, anche, alla difesa della sovranità nazionale, in un contesto di progressiva proiezione del conflitto e del potere sul dato e su quella potentissima infrastruttura sociale che è la rete.

La stessa competizione per l'egemonia tecnologica cela, oggi, una più stretta connessione con le dinamiche geopolitiche, suscettibile di coinvolgere in maniera determinante profili di sicurezza nazionale.

Condivisibile, quindi, la preoccupazione, espressa dal Copasir, per la possibile recessività delle esigenze di *cybersecurity*

rispetto agli interessi commerciali, che coglie fino in fondo le implicazioni proprie di un certo tipo di neo-imperialismo digitale.

Come sottolineato dal Consiglio Ue, tra i fattori di rischio correlati al 5G vanno infatti annoverati non solo i profili tecnologici, ma anche quelli ordinamentali.

Ciò impone, dunque, di considerare i rischi connessi alla fornitura di tecnologia da parte di aziende, quali quelle cinesi, inserite in un contesto di dirigismo (anche) economico che le obbliga a cooperare con il Governo, fornendogli pezzi importanti del proprio patrimonio informativo, con implicazioni da non sottovalutare sul piano della sicurezza nazionale.

In tale prospettiva abbiamo, peraltro, in più occasioni auspicato un "*Privacy Shield*" con la Cina, per garantire il rispetto di alcune basilari condizioni di tutela del diritto alla protezione dei dati (se non altro) dei cittadini europei.

Siamo consapevoli che un simile accordo necessiterebbe di una revisione radicale del sistema giuridico cinese, tale da escludere, in particolare, il prelievo sostanzialmente illimitato, da parte del Governo, dei dati nella disponibilità delle aziende.

E tuttavia la dimensione e l'incombenza dei rischi per la sicurezza dei nostri paesi non consentono né inerzia né, tantomeno, rassegnazione.

E in questa competizione sino-americana per l'egemonia sulla potenza di calcolo, l'Europa rischia di perdere ogni possibile ruolo, se non ha la forza di opporre, al *dumping* digitale, un'idea di innovazione democraticamente sostenibile, fondata su principi di trasparenza e responsabilità algoritmica e tale da coniugare economia e diritti, libertà e sicurezza. Che tornerebbero ad essere valori complementari e non antagonisti, quali del resto l'ordinamento europeo li delinea, nella consapevolezza di come la democrazia viva necessariamente di entrambi.

Sarà forse necessario aggiornare l'agenda politica, mettendo al centro idee e progetti per governare la società digitale nei prossimi anni, per garantire i diritti e le libertà in questa nuova dimensione della vita: la protezione dati può essere, in questa prospettiva, una bussola affidabile.

# **Spazio cibernetico bene comune**

## **Protezione dei dati, sicurezza nazionale**



**INTERVENTI DEI RELATORI**

**Raffaele Volpi**

**Arturo Di Corinto**

**Stefano Zanero**

**Gabriele Faggioli**

# Sicurezza cibernetica e libertà individuale: una prospettiva comune

Raffaele Volpi  
*Presidente del Copasir*

---

Prima di tutto mi permetto di ringraziare il Presidente Soro per l'invito, per me è assolutamente un piacere, lo trovo anche un momento di grande responsabilità essere qua.

Mi permetto di salutare tutti i presenti, i componenti del collegio del Garante, i signori ufficiali e i direttori dei nostri servizi che, per loro disgrazia, mi onorano anche dell'amicizia. Io starei attento, però grazie ancora. Ancora di più per ringraziare, attraverso di loro, tutti coloro che lavorano quotidianamente alla sicurezza del Paese. Per l'amicizia, dicevo, ma anche per la proficua collaborazione con l'organo parlamentare, ma anche per la parte informale con la quale riusciamo quotidianamente a individuare le criticità legate alla responsabilità del Paese.

Ovviamente noi siamo un organo di controllo, però grazie anche, Presidente Soro, al mio predecessore si è trovato uno spazio di proattività maggiore rispetto a quella che poteva essere semplicemente una valutazione in ricezione di quello che succedeva. Questa è già la dimostrazione che - come lei rappresenta un'*Authority* - anche il Comitato parlamentare per la sicurezza della Repubblica nei suoi risultati non ha connotazione politica, ma ha connotazione di interesse nazionale. Questo tengo a specificarlo, perché abbiamo cose in comune con il Garante della privacy. Sicuramente gradi di riservatezza o segretezza nelle fasi istruttorie e certamente il fatto che quello che poi

esce come prodotto è un prodotto che ha una condivisione basata su elementi realistici, ovviamente non tutti palesabili, ma certamente di grande importanza per le valutazioni finali.

Presidente Soro, io la voglio ringraziare per le considerazioni che ha fatto nella sua relazione, che si sono tradotte già in questa settimana - ho visto - in indicazioni particolarmente specifiche su alcuni casi, su uno in particolare. Questo vuol dire avere il coraggio delle istituzioni, vuol dire l'implicazione delle istituzioni in maniera complessiva, vorrebbe dire - qui purtroppo uso il condizionale - che quello che viene detto da istituzioni come la vostra e magari più particolari come il Comitato per la sicurezza della Repubblica deve essere tenuto in considerazione nelle scelte politiche. Su questo non c'è dubbio.

Mi permetto alcune riflessioni. Sappiate tutti che io non sono un esperto, sono avventizio e *pro tempore*, e sicuramente non ho nemmeno l'eloquenza né del Presidente Soro né dell'amico Di Corinto. Cerco quindi semplicemente di fare due valutazioni. Prima è stato ricordato Rodotà. Io mi permetto di dire che Rodotà ha fatto tantissimo nella divulgazione della cultura di un certo tipo di idea della *privacy*, però ieri sera riflettevo che noi siamo passati in pochi anni dall'articolo 15 della Costituzione, sull'inviolabilità della corrispondenza, ad immaginarsi l'inviolabilità di dati che sono in un circuito addirittura mondiale.

Questa è la nostra sfida.

Presidente Soro, io la ringrazio ulteriormente perché lo sforzo che stiamo facendo, che voi state facendo e che avete già fatto è innanzitutto culturale legato alle generazioni, è legato al cambiamento della tecnologia. Tutti noi che operiamo sia a livello parlamentare, legislativo all'interno delle *Authority* o nella parte legata alla sicurezza del Paese ci siamo trovati nella necessità di individuare degli spazi nuovi.

Nella sua relazione c'era un chiaro legame fra la globalità degli interessi e la necessità che questi vengano individuati con molta chiarezza nella loro protezione; oggi purtroppo alcune

guerre sono ancora fatte in maniera tradizionale, ma è evidente che la grande sfida sono le guerre economiche, che vengono fatte attraverso tutto quello che è lecito e, in parte, anche con quello che non è lecito, quindi c'è una sfida legata ai mezzi. Però c'è una cosa che è precipua, che è quasi di inizio rispetto alle nostre necessità: i Paesi - ovviamente noi parliamo dell'Italia - devono entrare in una fase di consapevolezza. La consapevolezza è legata, dal mio punto di vista, a due passaggi. Scusate se sono schematico, ma credo che queste cose debbano essere ben percepite, forse meno da noi che ci operiamo quotidianamente ma dal mondo esterno e anche da chi fa attività politica.

L'interesse nazionale non è più quello individuabile semplicemente come quello dello scorso secolo. Non è più vero che l'interesse nazionale è legato a dei confini certi.

Il nostro interesse nazionale è legato a tutto quello che riguarda l'economia del nostro Paese. Quindi può essere - e lo dico casualmente in questi giorni - una piattaforma dell'ENI, ma può esserlo assolutamente un interesse economico dall'altra parte del mondo. Quindi in questo caso l'interesse nazionale e la sicurezza nazionale, specialmente per i settori strategici, a volte collimano e non sono più necessariamente circoscritti all'interno di un confine nazionale. Questo è lo sforzo che stiamo facendo tutti nell'individuazione dei perimetri di sicurezza.

Ieri, se non sbaglio, sono uscite le raccomandazioni europee sulla sicurezza cibernetica. Le aspettavamo il 31 dicembre, sono state pubblicate ieri. Questo è un primo indirizzo che dovrebbe però portarci ad un ragionamento più complessivo, che è già stato citato dal Presidente: quali sono i confini dell'intervento possibile. Se noi partiamo da quell'idea dell'inviolabilità della corrispondenza, arriviamo oggi a un'intrusione continuativa, che però - va detto - è in parte consapevole (chiunque di noi usa un *social* sa che c'è un utilizzo della nostra profilatura). La cosa che diventa un pochino più preoccupante è un aspetto legato a qualcosa che è diverso dalla necessità del mercato. Qui ci si lega a una cosa centrale.

Vedete, io sono profondamente legato a dei valori occidentali che parlano comunque di libertà, parlano di individuo; se qualcuno cerca di vendermi un prodotto, ci posso stare, lo capisco, ma nel momento in cui la profilatura diventa sociale, quindi ingegneria sociale, quindi condizionamento delle scelte, non ci sto più. Questo vuol dire che, se i miei valori non coincidono né con i mezzi né con i sistemi, devo fare qualcosa di estremamente deciso rispetto a un'intrusione che è qualcosa di diverso. Mi permetto di dire, in alcune aree del mondo, magari meno avanzate rispetto ai livelli economici ma molto più influenzabili, si usano i mezzi tecnologici al fine addirittura di condizionare delle scelte che poi diventano di massa. Non sto parlando di voti ma di migrazioni. Io non sono abituato a parlare di immigrazione, quindi mi fermo qua, per dire che le capacità economiche di chi interviene a livello di ingegneria sociale sono talmente alte, per cui se un Paese come il nostro, consapevole, pieno di valori e di storia, non ha la capacità di entrare nella fase della consapevolezza, diventa un problema.

Io credo che ci siano altre cose. Penso che tutto quello che noi facciamo a livello di *privacy*, ma che poi è sicurezza, è piacere dell'individuo e non intrusione sull'individuo, stia all'interno di quella concezione, che è già stata citata - l'ho citata anch'io -, che è valoriale. Non è vero che le scelte che si fanno in cose che possono sembrare parcellizzate, ovvero oggi parliamo di *privacy*, domani parliamo di sicurezza, dopodomani parliamo di aeroplani, sono al di fuori di una concezione più generale. I Paesi come il nostro hanno il vantaggio della possibilità di operare in termini di multilateralismo, ma certe scelte sono strategiche e geopolitiche.

I Paesi devono sapere con chi stare, come starci e con che mezzi starci. Quindi la carenza inevitabile è quella di individuare non solo tecnologicamente i confini di protezione.

Io penso che l'Italia abbia già fatto un passo avanti con le leggi sul perimetro di sicurezza, con la "Golden Power", ma credo che sia quasi impossibile ragionare in termini nazionali.

L'Europa ieri ha tracciato una serie di raccomandazioni.

Io ritengo che alcune cose non possano essere solo raccomandazioni, che ci debba essere una trasformazione più profonda fra i Paesi che collaborano; penso che ci debbano essere perimetri di sicurezza che vadano anche sovrapposti, per esempio, a quelli dell'Alleanza atlantica con i protocolli comuni; e credo che non si possa immaginare, per esempio, che le azioni fatte dal Copasir, così come per il Garante, possano essere necessariamente contro qualcuno. Io so che ci sono degli interessi importanti, però vorrei insistere su un fatto: se le nostre organizzazioni sottolineano delle criticità, non lo fanno semplicemente perché debbono andare contro qualcuno, contro qualche Paese, ma perché ci sono delle evidenze.

Prima è stato citato un passaggio sulle preoccupazioni del futuro. Siamo già avanti, però facciamo un'ipotesi. Quindici giorni fa su *Twitter* ho visto un annuncio della Repubblica cinese che riportava: "Oggi è stato testato per la prima volta un satellite quantistico. Avevamo dei problemi nelle stazioni di ricezione che erano troppo grosse, abbiamo trovato la soluzione, adesso la capacità della stazione di ricezione dal satellite alla rete quantistica è ridotta a una valigia.

Per la prima volta - lo dicono loro, quindi mi fido - da questo satellite con sistema quantistico abbiamo mandato la prima rete che abbiamo sul territorio dei dati criptati". Mi sembra una bella cosa.

Il futuro anche di altri sistemi di difesa d'arma ormai è trагuardato al quantistico, io sono un provinciale, quindi non parlo di metropolitane, di cose complesse, però mi è venuto in mente: e se nel mio paesello di campagna qualcuno pensasse domani, attraverso una rete informatica non protetta, attraverso la trasmissione di un dato quantistico su una valigetta, di fermare l'elettricità, cosa facciamo? So che è un po' fumettistica la cosa, ma credo che non lo sia poi così tanto. Quindi, se noi non impariamo a tradurre gli aspetti del vantaggio economico, che non sempre c'è, rispetto allo sviluppo del Paese, ma ci mettiamo anche quella che

è la sensibilità sulla nostra sicurezza, Presidente, possiamo tradurre una volta ogni tanto la parola “sicurezza” in “libertà”? Possiamo tradurre la parola “sicurezza” nel fatto che la mia sicurezza, la nostra sicurezza non è semplicemente un dato utopico o astratto, ma è la mia personale libertà di fare delle scelte? Di poter vivere con una tranquillità sociale, di sapere che i condizionamenti sono limitati a quello che io scelgo di avere come condizionamento?

Se così non fosse, vuol dire che non abbiamo capito nelle nostre scelte future, anche quelle politiche, anche quelle di sicurezza, la differenza fra l’attualità e il passato. Il passato era la lettera, oggi c’è qualcosa di diverso.

Il discrimine in questa cosa di diverso è materiale e immateriale. La lettera era dato materiale. Oggi il materiale e l’immateriale si distingue fra la rete e le cose che passano sulla stessa. Se noi non capiamo l’elemento valoriale della libertà, il discrimine fra rete e dati, temo che difficilmente riusciremo a raggiungere un grado di sensibilità tale da essere estremamente fermi nelle scelte che dobbiamo fare come Paese.

Penso oltretutto che queste cose dovrebbero essere al di fuori della sensibilità particolare dei partiti. La mia fortuna è di essere un presidente di opposizione. È l’unico organo che elegge un presidente di opposizione. Però per esempio il rapporto trasmesso al Parlamento rispetto alle nuove tecnologie è stato votato da tutti i componenti del Comitato, quindi vuol dire che c’è materiale abbondante per arrivare a quelle conclusioni. Io credo che non possa essere messo in un cassetto.

A una certa ora vi dovrò lasciare, perché ho il piacere di avere in audizione il Ministro dello sviluppo economico, Patuanelli, che credo su questa materia abbia delle considerazioni interessanti da fare, perché la mia opinione è che non si vende la libertà. La libertà che abbiamo conquistato non si vende per qualche centinaio di milioni di euro.

La nostra libertà vale qualcosa di più, e io penso che le scelte economiche stiano in quella serie di valori e identità

che sono state citate prima. Valori e identità che vogliamo dire libertà individuale.

Noi oggi abbiamo una responsabilità, Presidente, che qualche volta fuori non è percepita. Il nostro lavoro è straordinario, quello che fanno le forze dell'ordine, che fanno i servizi, che fate voi, perché noi siamo ormai abituati a ragionare in termini di massa, ma il nostro piccolo, modestissimo lavoro è fatto sull'individuo. Nel momento in cui io agisco sulla comunità dando questo spazio di certezze e di serenità, lo faccio per il Paese, ma il Paese siamo noi: non siamo una cartina geografica, siamo persone che tutti i giorni hanno e devono avere la possibilità di poter scegliere. Io questa capacità di poter scegliere vorrei continuare ad averla.

La cultura occidentale non è contro lo sviluppo: lo sviluppo dovrebbe essere, anzi, l'elemento prioritario. Però lo sviluppo si fa anche con la cultura, e la cultura ha dei principi che nascono dalla nostra storia.

La mia preoccupazione, la nostra preoccupazione è semplicemente una: mai nessuno di noi penserebbe di fare azioni di distorsione di mercato: non tocca a noi, non tocca al Comitato, non tocca al Garante. Credo che ci siano forme di distorsione di mercato che dovrebbero arrivare addirittura al WTO. Credo che questa sia l'azione politica che la stessa Europa debba fare.

Sapete tutti che noi abbiamo dei problemi, non sono nemmeno dei problemi, sono un dato di fatto: gli aiuti di Stato non sono permessi. Ci sono due considerazioni, traggo spunto da una notizia uscita sull'*Handelsblatt* che ha dato rilievo alla notizia che dagli Stati Uniti d'America sia arrivata la conferma che le aziende cinesi, che producono *hardware* e *software* per le reti di quinta generazione, riportano esattamente tutto quello che fanno al Governo cinese per la legge che lo prevede; quindi hanno introdotto un ulteriore elemento di preoccupazione rispetto alla penetrazione del 5G in Europa. *Huawei* è obbligata a dare i dati al Governo cinese? No, non lo penso nemmeno io.

Però penso che, se un'azienda ha quelle che possono essere delle forme di aiuti di Stato, prima o poi le viene chiesto di ritornarli in qualche modo. Questo è un mio pensiero, perché chiaramente, se io faccio cablaggi in una città che costano dieci, me ne pagano cento, secondo me è aiuto di Stato. Non sto parlando di *Huawei*, sto parlando ipoteticamente di qualsiasi forma di aiuto di Stato.

Ci sono i metodi. Antonello, posso fare una brevissima digressione? Come Comitato abbiamo deciso di iniziare un'indagine, come forse qualcuno di voi ha letto, sui settori economici (bancario, assicurativo, energia e difesa): a me interessa capire come gli altri arrivano in Italia. Non è un problema semplicemente economico, ma se tu utilizzi in Italia dei metodi che non sono legali per condizionare magari i consigli d'amministrazione o scelte economiche, tu in Italia non ci puoi stare. E io non penso che il nostro Paese possa consentirsi, anche all'interno di sistemi come quello bancario o assicurativo, se non in certezza di diritto rispetto a quello che succede sull'*e-governance*, di permettere a qualcuno di condizionare all'interno di questi grandi istituti, che hanno miliardi di titolo sovrano “in pancia”, di fare scelte che non sono nell'interesse nazionale. Quindi tutto rientra nell'interesse nazionale.

Non siamo contro nessuno, io sono per il libero mercato, però in Italia innanzitutto non si mente e, se il Garante dice delle cose e se il Copasir dice delle cose, non se le è inventate al mattino, ricordando ancora una volta che il Copasir ha iniziato questa indagine con un presidente del Partito Democratico che è attualmente Ministro della difesa, lo presiede ora un esponente della Lega e il documento è votato da tutti i componenti che sono di tutti i partiti. Quindi io posso anche capire che ci siano delle difficoltà, ma non sono ostative rispetto allo sviluppo, sono però ad alcune certezze che non ci sono state.

# Data commons. Privacy e cybersecurity sono diritti umani fondamentali

Arturo Di Corinto

*Giornalista esperto di cybersecurity*

*Autore e inviato di "Codice" - Rai1*

---

La *privacy* è come la libertà: se non gli dai valore, rischi di perderla. Già. Nonostante l'eco mediatica e gli interventi resi possibili dal nuovo Regolamento europeo sulla privacy, il Gdpr, sono ancora in tanti, troppi, a non dare valore ai propri dati personali. Ma quei dati identificano comportamenti quotidiani e permettono di profilare gli utenti digitali indirizzandone scelte e azioni. E così, come dice lo storico Noah Yuval Harari "La gente è felice di elargire la propria risorsa più preziosa - i dati personali - in cambio di servizi di posta gratuiti e video di gattini. Un po' come è accaduto agli africani e agli indiani d'America che hanno venduto grandi territori in cambio di perline colorate" (*21 Lezioni per il XXI secolo, 2018*).

I dati sono l'oro e il petrolio dell'umanità connessa e dalla loro corretta gestione dipendono i gradi di libertà delle scelte quotidiane. E allora perché siamo pronti a darli via solo per partecipare a sonore litigate su *Facebook*, farci buggerare via email da rapinatori digitali e tracciare da poliziotti zelanti con *app* pensate per i criminali? La verità è che nella gestione della propria presenza online si rivela quel pericoloso divario digitale che ancora oggi, a 30 anni dal *web*, riflette antiche disuguaglianze: tra chi è capace di controllare, difendere e rivendicare la tutela dei suoi dati e chi non è in grado di farlo.

Potremmo sbrigarcela dicendo che con gli *smartphone always on* e le *app* a prova di incapace abbiamo messo armi potentissime in mano ad adulti che si comportano come bambini che bisticciano, tifano, si mostrano crudeli verso gli altri, dimentichi di ogni forma di empatia. Ma non possiamo.

Questa ignoranza digitale indirizzata dal mercato è il frutto di vari fattori: la diffusione su scala globale di *personal media* sempre più potenti, maneggevoli ed economici; un sapere comunicativo diffuso promosso da scuole e università; l'iperconnessione religiosa ai social; l'avvento della *me-communication*, la “comunicazione autoriferita”, come la chiama il sociologo Manuel Castells (*Comunicazione e Potere, 2009, 2017*). Pilotata dai signori delle piattaforme che oggi sono i signori dei dati, l'ignoranza digitale ha generato un nuovo Feudalesimo digitale (*Paul Mason, Il Futuro migliore, 2018*), che divide il mondo in due, tra chi produce gratuitamente questi dati e chi li raccoglie e mette a profitto.

La raccolta, l'organizzazione e l'utilizzo dei dati sono al centro del capitalismo estrattivo delle piattaforme (*David Harvey 2004, Carlo Formenti 2008, Shoshana Zuboff 2019*) che, conoscendo le più intime inclinazioni, il *sentiment*, dei propri utenti, sono in grado di anticiparne mosse e desideri affinché continuino a produrli. Prodotti e trattati da algoritmi potenti, con le metodologie delle scienze sociali (la psicometria), diventano il carburante per le intelligenze artificiali che ci sostituiranno (già lo fanno) in compiti complessi per i quali una volta si veniva remunerati e campavano le famiglie.

La violazione dei dati realizzata da *Cambridge Analytica* per cui *Facebook* è stata multata - facendogli il solletico - rientra in questo schema: se conosco gli orientamenti politici del produttore di dati - e lo so in base ai *like* che ha messo - sarò in grado di cucirgli addosso un messaggio che non potrà rifiutare. Il messaggio andrà a rinforzare le sue convinzioni preesistenti e gli stenderà intorno un “cordone sanitario” affinché non acceda a contenuti che le possano mettere in discussione (*Quattrociocchi, Vicini, Liberi di crederci, 2018*).

## I termini di servizio della nostra vita *onlife*

Quando ci iscriviamo a un sito, *app* o servizio Internet, in genere ci viene richiesto di accettare i «Termini di servizio», i ToS, che indicano come i nostri dati sono raccolti e usati. La maggior parte delle volte non li leggiamo, semplicemente perché non ne abbiamo il tempo e la voglia, ma soprattutto perché non li capiamo, visto che sono scritti in legalese.

Eppure è così che perdiamo così il controllo dei dati che ci identificano come cittadini, lavoratori e consumatori. Quei dati infatti verranno utilizzati per creare dei profili dettagliati dei nostri comportamenti e verranno commercialiati per usi che non sempre conosciamo. Ad esempio i ToS di *Facebook* ed *Amazon* dicono che i nostri dati sono usati per tracciare il nostro comportamento su altri siti, *LinkedIn* raccoglie, usa e condivide i dati di geolocalizzazione e *Instagram* ci mette il *copyright*.

I termini di servizio di *Reddit*, *Yahoo* e *WhatsApp* dicono che usandoli accettiamo «di difendere, indennizzare e sollevare il servizio da ogni responsabilità in caso di reclamo». Quasi tutti prevedono che gli stessi termini possono essere modificati in qualsiasi momento a discrezione del fornitore, senza preavviso per l'utente.

Nel suo Data Manifesto, Kevin Kelly, tecnologo e co-fondatore della rivista *Wired*, dice che i dati «non esistono da soli», che hanno valore solo se messi in relazione ad altri dati e che circolando diventano una risorsa condivisa. Per questo possono risentire della tragedia dei beni comuni, cioè di un'egoistica azione di appropriazione - come quando un privato recinta un pezzo di parco pubblico - e pertanto vanno protetti dai governi.

Ma i dati sono un bene comune perché, sulla base dei dati raccolti, possiamo costruire una società migliore. I dati che noi produciamo incessantemente attraverso l'interazione con i dispositivi digitali, rappresentano comportamenti quotidiani e possono essere una base di conoscenza importante per sviluppare politiche efficaci, servizi utili alle persone e nuovi prodotti. I dati, anonimizzati e

aggregati, possono servire a migliorare la capacità di uno Stato di rispondere alle esigenze dei propri cittadini.

Due esempi. Se noi abbiamo i dati, anonimi e aggregati, dei pazienti ospedalieri, probabilmente saremo in grado di pianificare meglio le risorse sanitarie necessarie a garantire la salute pubblica. Già viene fatto, pensate agli sforzi di raccolta e analisi dei dati epidemiologici.

Se abbiamo i dati di quanti e quali attacchi cibernetici ci sono stati negli ultimi anni, saremo sia in grado di anticipare nuovi attacchi che di imparare a difenderci. Quindi, il dato inteso come bene comune è questo: è un dato che può essere utilizzato in maniera utile dagli Stati per consentire una migliore qualità della vita delle persone e garantire diritti all'altezza delle democrazie in cui vogliamo vivere.

Il Gdpr, il Regolamento europeo generale sulla protezione dei dati prevede, in caso di grave violazione dei *database*, la comunicazione diretta ai singoli interessati entro 72 ore, pena multe salatissime, fino a 20 milioni di euro e al 4 per cento del fatturato annuo aziendale. Le sanzioni possono essere un deterrente, ma non lo sono per i grandi *player* della rete.

Perciò anche noi dobbiamo fare la nostra parte e capire se, quando e come ci conviene cedere i nostri dati.

### ***Privacy e cybersecurity sono diritti umani fondamentali***

Ma c'è un'altra questione, il rapporto stretto che lega la *privacy* alla *cybersecurity*. Il motivo è semplice da capire: in un mondo digitale i dati che identificano i nostri comportamenti sono digitalizzati; se non riusciamo a tutelare questi dati digitali, non riusciamo a tutelare i nostri comportamenti. In particolare non riusciamo a tutelare i comportamenti passati dalle tecnologie che li possono spiegare e dalle tecnologie che li possono predire. I dati personali sono uno strumento di *intelligence*. Pensiamo alle massive violazioni di basi di dati personali usati per orientare il comportamento delle persone.

Con i dati ormai ci si fa la “guerra”.

Però, se la *privacy* è l'altra faccia della *cybersecurity* è anche vero che la *privacy* è un diritto fondamentale dell'Unione Europea, mentre la *cybersecurity* non lo è. Eppure, in un mondo in cui ogni comportamento viene datificato diventando un dato digitale, proteggere quei dati che rimandano ai comportamenti quotidiani è cruciale, lo ripetiamo, proprio per la loro capacità di spiegare i comportamenti passati e di predire quelli futuri.

Se non riusciamo a proteggere i dati che ci definiscono come cittadini, elettori, lavoratori, e vicini di casa, potremmo essere esposti a un potere incontrollabile, quello della sorveglianza di massa, della manipolazione politica e della persuasione commerciale. Pertanto *privacy* e *cybersecurity* sono la precondizione per esercitare il diritto alla libertà d'opinione, d'associazione, di movimento, e altri diritti altrettanto importanti. Se accettiamo questa premessa possiamo pensare alla sicurezza informatica dei nostri dati come a un diritto umano fondamentale.

### ***Privacy e anonimato***

Eppure. Mentre la Bbc decide di portare i suoi contenuti nel *Dark Web* per tutelare l'anonimato del proprio pubblico all'interno di paesi illiberali, in Italia si discute ancora di identificare gli utenti del *web*.

Il dibattito, che pensavamo chiuso dopo le mobilitazioni degli anni scorsi contro la censura in rete, è ricominciato per la proposta di un parlamentare di Italia Viva a suo dire preoccupato per il dilagare dell'odio in rete, e che ha suggerito, parole sue, di rendere obbligatorio depositare un documento d'identità prima di aprire un profilo *social* «per impedire che il *web* rimanga la fogna che è diventato».

Purtroppo questa risposta a problemi reali, l'*hate speech*, le *fake news*, il *cyberbulismo*, è sbagliata. Per vari motivi. Il primo è che molti odiatori in rete si presentano già con nome e cognome e il riscontro anagrafico non sarebbe un deterrente. Il secondo

è che nessuno in rete è veramente anonimo e non c'è bisogno della carta d'identità per risalire ai dati anagrafici dei bulli in rete nonostante abbiano uno pseudonimo.

Per farlo occorrono tempo e risorse, riuscirci non è facile né immediato, ma si fa quando serve. Viceversa l'identificazione in massa degli utenti è un processo tecnicamente complesso e oneroso.

Il punto è qui che gli odiatori che spesso si presentano con nome e cognome in genere sono persone che semplicemente non sanno che un insulto, una minaccia espressa online, può essere perseguita come se fatta a scuola o al bar. I «*flame*», i litigi in rete, inoltre, sono un elemento costitutivo della comunicazione virtuale: i *social* e i canali di *chatting* sono strumenti di dialogo veloce, dove si interagisce d'impulso, «luoghi» dove l'assenza fisica dell'interlocutore fa venire meno il timore della rappresaglia e spesso anche il pudore, la vergogna e la cautela nell'esprimere opinioni estreme.

Eppure la questione è più ampia. Il *web*, o i *social* che ne rappresentano una parte, non è fatto solo di maleducati, odiatori, bulli, *stalker*, per i quali in realtà ci sono leggi anche severe che ne puniscono i comportamenti. Il *web* usato in maniera anonima è anche il *web* dei dissidenti politici, dei profughi senza documenti, dei rifugiati, perseguitati nei loro paesi per essere omosessuali o per avere evaso la leva obbligatoria. E poi ci sono i cooperanti che vivono in zone di guerra, i *blogger* antimafia che non possono farsi riconoscere, e ci sono i *whistleblower*, i *citizen journalist*, gli impiegati di enti, ministeri e Forze Armate che devono gioco-forza assumere identità fintizie per evitare ritorsioni a fronte delle loro denunce.

In aggiunta ci sono soggetti fragili che per raccontare esperienze di abusi e maltrattamenti mai e poi mai vorrebbero presentarsi con nome e cognome. Quindi la domanda è: per provare a spaventare gli odiatori in rete è giusto cancellare l'anonimato di chi grazie ad esso può esprimersi liberamente? Senza anonimato

cadrebbero nell'autocensura e nel conformismo preventivo. E saremmo stati noi a togliergli quella tanto faticosamente conquistata libertà di parola. Le catacombe parlamentari sono piene di disegni di legge per limitare la libertà d'opinione in rete.

All'epoca della televisione erano tentativi surrettizi di mantenere la società divisa tra chi ha potere di parola e chi no, come diceva Michel Foucault. Ma oggi? Dal canto nostro preferiremmo che tante energie venissero impiegate per educare le persone al rispetto degli altri e perché no, anche al rispetto delle leggi che ci sono, e sono già abbastanza.

### **Anonimato, *fake news* e disinformazione**

L'anonimato in rete però permette anche di agire pratiche di disinformazione. Sappiamo che le strategie di disinformazione si basano sulla manipolazione delle percezioni. La disinformazione è un'arma per indurre l'avversario a fare delle scelte sbagliate. Le *fake news* oggi sono la testa d'ariete di queste strategie di disinformazione e servono a farci "comprare" quello che altri hanno deciso che "vogliamo" comprare: uno shampoo, una strategia, oppure un candidato politico.

Insieme alla profilazione dei *social network* le *fake news* pongono un problema molto serio anche alla sicurezza nazionale.

Una volta le campagne di disinformazione bersagliavano i decisori - funzionari pubblici di alto livello, i politici, i giornalisti affermati, i funzionari dello Stato -, oggi queste campagne di disinformazione sono dirette a manipolare quella forma larvale di dibattito pubblico che c'è sui *social network*. Come? Agendo attraverso la propaganda computazionale che sfrutta i *social media* e la credulità di chi li abita, la psicologia umana che non distingue la realtà dalla finzione, le voci e i pettegolezzi tanto cari ai cospiratori e gli algoritmi per manipolare l'opinione pubblica.

È così che funzionano i *dark ads*: messaggi promozionali a pagamento diretti solo a specifici indirizzi o territori.

I dati raccolti dalle piattaforme sono usati per creare profili individuali e collettivi. Questa profilazione può essere usata per comunicazioni mirate e geolocalizzate, anche durante le elezioni.

La logica qui è doppia: se so chi sei, so quali contenuti farti vedere. Se conosco le tue scelte passate sono in grado di mostrarti solo le notizie che sei pronto a cliccare. Ogni click dice quali sono le nostre preferenze culturali e politiche, proprio quelle che sono collezionate nei giganteschi *database* che i padroni dei dati come *Google*, *Amazon* e *Facebook* usano per definire i nostri profili sociali, economici, ed elettorali.

Quindi la manovra è a tenaglia: prima la profilazione e l'esposizione alle *fake news* per polarizzare l'elettorato, poi il messaggio politico ritagliato *ad hoc* sotto forma di una comunicazione nominativa, diretta a una moltitudine di singoli elettori, ai quali viene recapitata in maniera ripetuta un'informazione specifica e coerente con il proprio profilo psicologico ed elettorale.

Nell'era di Internet la disinformazione fa largo uso delle *fake news* e la sua viralità approfitta soprattutto di *Facebook*, *Google*, *Instagram* fino a *WhatsApp*, piattaforme che agiscono da potenti casse di risonanza per i nostri pregiudizi, soprattutto quando sono veicolati da chi ci fidiamo di più: amici e conoscenti.

Se la natura originaria delle bufale è quella di creare traffico *web*, e quindi macinare soldi dagli annunci pubblicitari, molti "spacciatori" di notizie false agiscono sotto falsa identità e hanno una motivazione ideologica: affermare un punto di vista anziché un altro, distorcere la realtà delle cose e creare "fatti alternativi". Una tecnica propagandistica salita prepotentemente alla ribalta durante la corsa alla Casa Bianca del 2016 ma che ha degli antenati "illustri" nelle *psy-ops*, le operazioni di guerra psicologica condotte da eserciti rivali per demoralizzare le truppe avversarie, influenzare il *sentiment* della popolazione e disorientare i governi. A produrre disinformazione ci sono oggi i gruppi di "nation-state hackers", chiamati anche APT (*Advanced Persistent Threat*), "minacce avanzate persistenti" che hanno come obiettivo di interfe-

rire con la democrazia. Si tratta di gruppi paramilitari cibernetici che vengono dai ranghi dell'*intelligence*, della polizia e dell'esercito, e hanno il compito, per conto dello Stato a cui hanno giurato temporanea fedeltà, di raccogliere informazioni su aziende concorrenti, su Stati avversari, su decisori pubblici per orientarne i comportamenti. Possono anche compiere azioni di sabotaggio o di guerra cibernetica. Perché? Per destabilizzarne l'economia o indebolire un avversario, ma anche per realizzare operazioni psicologiche orientate a creare malumore, diffidenza o paura nelle popolazioni, facendo uso di informazioni fasulle su *target* ben individuati.

Ecco, le campagne di disinformazione orchestrate dagli APT si basano sulla conoscenza del *target*, sui dati da essi prodotti, e servono a indirizzare le percezioni e le scelte maturate nell'*agorà* pubblica del *web*.

Quindi non vanno solo tutelati i dati personali in quanto tali, ma i dati che contribuiscono a definire la nostra persona digitale e che “rappresentano” scelte e desideri.

### ***Data Breach e banche dati***

Ovviamente sono i *data breach* il pozzo principale a cui attingono i delinquenti, i cybercriminali e gli APT. Nel dicembre 2019 abbiamo saputo che la banca Unicredit era stata violata o, meglio, che tre milioni di profili dei suoi clienti erano stati violati a seguito di un attacco informatico avvenuto nel 2015. Ma che dire della violazione delle PEC di cinquecentomila indirizzi relativi ai Ministeri che afferiscono al CISR (Comitato interministeriale per la sicurezza della Repubblica) avvenuto nel 2018?

Sicuramente c'è un tema che riguarda la formazione, la consapevolezza, ma anche la preparazione ad affrontare questi attacchi per tutelare la *privacy* di tutti: “non chiederti se verrai attaccato ma quando”. Un concetto altrettanto importante di quello di resilienza, la capacità di ripartire dopo uno *shock*, in questo caso informatico.

## Le infrastrutture critiche e la *privacy*

Se non è ancora chiaro, possiamo pensare al fatto che un attacco informatico di successo non solo può impossessarsi dei dati dei contribuenti, dei risparmiatori, dei legislatori, ma può determinare l'interruzione di servizi essenziali e bloccare la produzione industriale e mettere a rischio l'incolumità stessa di cittadini. Immaginatevi che cosa potrebbe succedere se ad un certo punto si spegnessero contemporaneamente in una grande città italiana i semafori, si bloccassero le operazioni chirurgiche, le ambulanze non ricevessero più le comunicazioni per andare a prendere i feriti. Cose del genere sono già successe.

Nel 2013 ci fu il tentativo di aprire le chiuse della diga di New York utilizzando un telefonino. L'Estonia e l'Ucraina hanno subito il *blackout* della griglia elettrica a seguito di un attacco informatico. In realtà gli esempi potrebbero continuare all'infinito. Se ricordiamo la minaccia Mirai, la *botnet* che bloccò per quasi un giorno intero le comunicazioni dagli Stati Uniti verso l'Italia, per 18 ore non fu possibile raggiungere i computer che ci permettevano di accedere al *New York Times*, a *Twitter*, a *Netflix*, *Amazon* e così via. Gli attacchi cibernetici sono sempre più pericolosi: in una società digitalizzata e iperconnessa, sempre più dipendente dalla tecnologia, gli attacchi cibernetici possono fare danni enormi.

## Perimetro nazionale

Con l'obiettivo futuro di proteggere dati e informazioni l'Italia ha selezionato una squadra nazionale di *hacker*. Sono i futuri *cyberdefender*, scelti da scuole e università attraverso la *Cyberchallenge*. L'Italia ha il *Golden Power*, cioè speciali poteri di voto nei confronti di produttori e tecnologie, come il 5G, che possono rappresentare un pericolo per la democrazia e l'economia della penisola.

L'Italia ha pure un «*Internet kill switch*». Significa che in presenza di un rischio grave ed imminente alla sicurezza nazionale causato dalla vulnerabilità di reti, sistemi informativi e servizi

informatici, il Presidente del Consiglio può disporre la disattivazione, totale o parziale, di Internet. Con le necessarie garanzie di legge. Una possibilità remota, ma prevista dalla legge sul Perimetro nazionale di sicurezza cibernetica.

La legge chiarisce la costante e contemporanea evoluzione dell'assetto cibernetico italiano, la «postura», si dice in gergo, e la mette in relazione con alcuni fattori di crescita e di innovazione che in una società aperta, digitale e iperconnessa, possono trasformarsi nel loro contrario e diventare vere e proprie minacce: cioè gli algoritmi di intelligenza artificiale, la crittografia e l'informatica quantistica.

Settori su cui l'Italia dovrebbe investire di più.

E tuttavia ci ricorda che la legge sul Perimetro nazionale, grazie al raccordo con la normativa sul *Golden Power*, alla nascita del Centro di Valutazione e Certificazione Nazionale, al futuro Csirt per rispondere prontamente alle emergenze, e ai poteri speciali di intervento, l'Italia è in grado di «affrontare con la massima efficacia e tempestività situazioni di rischio grave e imminente per la sicurezza nazionale in ambito *cyber*».

Il grande lavoro svolto dal Dipartimento informazioni per la sicurezza, DIS, ha favorito la realizzazione della legge sul Perimetro nazionale di sicurezza cibernetica. Nelle audizioni precedenti alla conversione della legge è stata detta una cosa molto importante, che il “rischio zero” non esiste e che tutti quanti noi ci dobbiamo impegnare affinché non accada che un ragazzino diciottenne dall'India possa fermare i treni che viaggiano in Italia.

Quindi se la *privacy* è un diritto fondamentale nell'Unione europea, lo è anche la *cybersecurity*, la tutela di dai, reti e informazioni sono la precondizione per esercitare altre diritti come diceva a proposito della *privacy* Stefano Rodotà: il diritto di associazione, di espressione, di opinione, di movimento e così via.

C'è una frase che viene attribuita anche a un presidente americano di nome Thomas Jefferson, che dice «Chi pensa di rinunciare alla propria libertà per avere maggiore sicurezza, non merita né la libertà né la sicurezza». Voleva dire che l'equilibrio

nelle scelte che facciamo per garantire sia la libertà sia la sicurezza dovrebbe essere l'oggetto della nostra attenzione.

Il nostro Paese, a cominciare dal decreto Monti, successivamente con il decreto Gentiloni, la legge sul Perimetro nazionale, il recepimento della direttiva NIS, del regolamento GDPR, l'allineamento del lavoro del nostro Parlamento con il *Cybersecurity Act* europeo, ci ha permesso di rimanere saldi in questo equilibrio tra *privacy* e *cybersecurity*. Bisogna continuare così.

Negli ultimi anni gli Stati si sono distratti e hanno lasciato che poche multinazionali avessero più dati sugli italiani di quanti ne ha il Governo che protegge gli italiani. Il tema della sovranità digitale diventa il *trait d'unon* fra la questione della *privacy* e la questione della sicurezza dei dati personali, comuni, aziendali, perciò non ci si può dire sovranisti senza pensare alla sovranità tecnologica e digitale.

# Cybersecurity e privacy nel futuro iperconnesso

Stefano Zanero

*Professore Associato, Politecnico di Milano*

---

Grazie allo spunto del moderatore della giornata di studio, Arturo di Corinto, siamo partiti da una definizione corretta del termine “*hacker*”, che è originariamente un termine buono o quanto meno neutro, che corrisponde, anche etimologicamente, al simpatico termine italiano “smanettone”.

Se si vuole intendere chi viola computer e reti al fine di guadagnarci, o di danneggiarli, si deve usare qualche aggettivo qualificativo, ad esempio *black hat hacker* o *malicious hacker*. Meglio ancora sarebbe chiamarli “*attacker*” o aggressori, perché la maggior parte dei criminali informatici non sono necessariamente degli *hacker*. È filosoficamente importante ricordare questa etimologia, ho il piacere di guidare uno di questi team di “smanettoni” nel mio laboratorio.

Ci sono varie università in Italia che per fortuna stanno promuovendo la ricerca nella *cybersecurity*, oltre al Politecnico mi piace citare i colleghi di Sapienza, di Padova, Verona, Venezia, che hanno contribuito molto a sviluppare tra le altre cose il programma della *CyberChallenge* ([www.cyberchallenge.it](http://www.cyberchallenge.it)). Questo programma mira a sviluppare giovani talenti, addestrandoli come *hacker* etici, allenandoli (come fossero una piccola “nazionale”) per partecipare alle competizioni europee di “*Capture the flag*”, un particolare torneo di abilità informatica dove le squadre dei diversi Paesi si affrontano per entrare nel fortino digitale di quell’altro e impedire all’avversario di entrare nel proprio.

Ovviamente, al di là del gioco, imparano anche le basi

tecniche che servono per formare i futuri difensori informatici del nostro perimetro cibernetico nazionale.

Qual è lo scenario che si troveranno di fronte questi nostri ragazzi (e noi) nel prossimo futuro?



Il nostro è un futuro che, prendendo un termine dai futurologi americani, è iperconnesso, un futuro dove, per funzionare, la società avrà sempre più oggetti dotati di intelligenza e distribuiti.

Un primo esempio potrebbe essere una *self-driving car*, un'auto che si guida da sola: ha ovviamente un'intelligenza a bordo per poter reagire prontamente al cambiare delle condizioni ambientali, ma anche una connessione profonda con un “*back end*” che colleziona una serie di informazioni, sulla base delle quali sono state apprese regole che fanno sì che questa cosa sia possibile. Quindi la presenza a bordo del veicolo di strumenti *smart* e la sua connessione al mondo di internet sono le due caratteristiche che rendono o renderanno possibile in futuro avere un'auto a guida autonoma.

Già ora, comunque, qualsiasi automobile moderna contiene tra i cinquanta e i centocinquanta *computer* collegati tra di loro da una rete uguale in natura alle reti che abbiamo nei nostri uffici, quindi è un *data center* che accidentalmente ha quattro ruote, un motore e un volante.

Questo *data center* è il meccanismo con cui siamo riusciti a fare veicoli più efficienti ma anche più sicuri, veicoli che ci proteggono, veicoli che sono in grado di intervenire sulle nostre decisioni in maniera per ora molto *soft*, ma nel futuro con una sempre maggiore autonomia.



La stessa cosa vale in tutti i campi della società. Facciamo qualche esempio.

Nella seconda immagine potete vedere un collega del Politecnico (Andrea Zanchettin) che lavora con un *robot* della multinazionale ABB, che si chiama YuMi. YuMi è diverso dai grandi *robot* delle catene di montaggio, perché è un *robot* cooperativo, fatto per non essere chiuso in una gabbia lontano dagli operai, ma per lavorare vicino fisicamente alle persone.

Per rendere sicura questa cosa, è necessario che YuMi sia dotato di tutta una serie di sensori: quella barra nera che vedete è una telecamera che fa in modo che il robot non possa interagire male con il suo collega umano, ma sia assolutamente sicuro da utilizzare.

C'è un'intelligenza distribuita all'interno della fabbrica che fa sì che i *robot* cooperativi come YuMi possano diventare dei compagni di lavoro per delle fabbriche intelligenti che sono ormai cosa del presente, neppure del futuro.



Tutti questi sono esempi di ciò che viene chiamato in gergo “*internet of things*”, che non vuol dire nient’altro che mettere potenza di calcolo all’interno dei dispositivi e poi collegarli tra di loro.

È una cosa che già succede, e che diventerà sempre più pervasiva e più trasparente per noi. Andiamo verso una società dove i dispositivi si parlano tra di loro, e noi ne vediamo gli effetti. Questa cosa è già presente. Un esempio comune è questo: quando prendiamo in mano il cellulare, una delle cose che ci vengono proposte è il punto dove abbiamo parcheggiato la macchina. Ma nessuno di noi ha segnato questo punto, né ha impostato alcunché per farlo capire. Semplicemente, basandosi sul *machine learning*, il sistema ha appreso che c’è un ricevitore *bluetooth* a cui il vostro cellulare si collega (e poi si scollega), e basandosi sull’analisi di come funzionano i cellulari di un miliardo di persone, si sa che quella sequenza succede durante lo spegnimento e l’accensione di un veicolo. Quindi, quando accade, il cellulare segna la posizione perché tira a indovinare, ma con ragionevole certezza, che quello è il punto dove avete parcheggiato la macchina.

Questa cosa non succede perché noi gliel’abbiamo insegnata, ma perché il cellulare registra una serie di informazioni,

le trasmette in rete, e poi queste informazioni vengono analizzate per estrarre dei *pattern* comuni. Ogni sera il cellulare sulla base dei miei spostamenti abituali mi propone la strada per tornare a casa, ma il venerdì mi propone la strada per andare a casa dei miei genitori, perché molto spesso il venerdì sera vado a cena da loro.

Queste piccole semplificazioni della vita quotidiana sono pagate da un prezzo molto caro in termini di raccolta ed aggregazione di dati su sensori che fino a qualche anno fa non ci saremmo neanche sognati di avere.



L'ingresso della tecnologia nella nostra società è pervasivo, difficile da fermare, da governare e, come il Presidente Soro giustamente nel suo intervento diceva, richiede una riflessione che va al di là della tecnologia, perché serve che in qualche misura la tecnologia venga governata in modo tale da poter contribuire, e non detrarre, dalle nostre libertà e dalla nostra capacità di agire e di prendere decisioni.

Questa cosa non è mai tanto evidente quanto se andiamo ad analizzare l'impatto, per esempio, che i *social network* hanno sulla nostra società, perché l'interazione tra la base di dati che noi forniamo e la base di dati che viene raccolta dalle nostre interazioni con gli altri è abbastanza difficile da stimare per tutti noi.

Se volete fare un esperimento, se avete un profilo *Facebook*, potete andare a leggere i dati che *Facebook* ha raccolto basati su terze parti, cioè non su quello che avete fatto su *Facebook* ma che ha comunque aggregato nel vostro profilo (<https://www.facebook.com/off-facebook-activity>).

Troverete elencate un sacco di cose che non pensavate nemmeno che avessero un'interrelazione con *Facebook*, e che dicono un sacco di cose di voi. Un sacco di cose che magari volontariamente non avete mai postato su *Facebook*.

Un altro esempio è il fatto che i nostri *like* e le nostre interazioni con i messaggi e con gli stati degli altri rivelano cose di noi che non abbiamo volutamente pensato di rivelare: dalle passioni politiche all'orientamento sessuale, tutti dati che una volta avremmo messo nella categoria di "dati sensibili", possono essere derivati dalle nostre interazioni ingenui con la "*internet of things*", vuoi con i *social network*.

Questo è il futuro iperconnesso che abbiamo davanti, dove il bilanciamento tra *privacy*, sicurezza e funzionamento della società è molto critico. È difficile da immaginare per il tecnologo ed è difficile da immaginare nel dialogo con chi invece si occupa della parte giurisprudenziale, della parte di analisi di decisione politica.



Se noi analizziamo le minacce informatiche, abbiamo un'evoluzione di queste minacce parallela all'evoluzione di come l'informatica è annidata nella nostra società.

Partiamo dalle minacce che riguardavano il *computer* e i dati, che sono quelle di cui ci siamo occupati per un sacco di tempo. Un esempio, riportato sulle *slide*, è una schermata di uno dei *ransomware* (*malware* che cifrano i dati sul *computer* e poi chiedono il riscatto) più diffusi. Questi sono interessanti perché rappresentano, da un lato, il classico aggressore economicamente motivato (l'aggressore che vuole fare soldi). La maggioranza degli aggressori informatici è economicamente motivata. La fetta restante è motivata da emozioni o da ideali di vario tipo, ad esempio politici o strategici.

Ad esempio, negli anni abbiamo avuto un sacco di episodi di “*activism*” o di rappresaglia tra organizzazioni più o meno statali o parastatali, e pezzi dello Stato.

Definire i confini di queste azioni diventa difficile, perché nel momento in cui c’è un sito di un Comune che è stato violato dagli *hacker from Golan*, cos’è questo? Un gruppo di ragazzini che si è divertito oppure è un’aggressione da un gruppo paramilitare a uno Stato? Il Comune in quel caso è semplicemente un sito che era poco protetto ed è stato aggredito o è un bersaglio che ha una significatività?



Non necessariamente lo sappiamo e non necessariamente è facile, nel mondo un po' nebuloso del digitale, capire esattamente questa cosa. Il sito del Comune è un pezzo di infrastruttura critica? Probabilmente no, ma magari per Comuni significativi potrebbe essere.



Alcune minacce non provengono da criminali informatici: prendiamo ad esempio uno Stato che esercita un suo sovrano tentativo di difendersi o di interagire con la sfera politica internazionale attraverso mezzi *cyber*. Dal punto di vista degli altri Stati, e dei cittadini degli altri Stati, è una minaccia.

Un esempio eclatante ci viene offerto dalle rivelazioni di Ed Snowden sui programmi della NSA. Quando è scoppiato il caso, non è che la comunità di quelli che si occupano di *security* sia caduta dalle nuvole: cosa facesse l'NSA lo sapevano tutti, è nella loro *job description*. Magari non ne conoscevamo appieno le dimensioni o la sistematicità.

Non voglio con questo sminuire l'importanza delle rivelazioni, che hanno trasformato sospetti in certezze. Tuttavia, era evidente e lo è sempre più che in una società digitalizzata, dove sempre più informazioni sul singolo cittadino sono disponibili in maniera molto granulare, l'intervento di un'agenzia (straniera) che

possa estrarle diventa una minaccia allo Stato nel suo complesso ed anche ad ogni singolo cittadino.



Questo si unisce all'osservazione che, siccome il nostro discorso politico nella società moderna si sposta in ampia parte sui *social network* e da essi viene mediato, ecco che diventa fondamentale capire l'influenza di campagne automatizzate di propaganda (ed anche l'influenza dello spostamento di mezzo in sé: *the medium is the message*). *Advertisement* che può venire comprato in maniera legittima è però ora così mirato sulla singola persona o su micro-popolazioni di persone che può avere un'efficacia non completamente studiata.

Questo è un grosso esperimento di cui tutti siamo le cavie da laboratorio. E chi ricorda come me la famosa “discesa in campo” di Silvio Berlusconi nel 1994, ricorderà i pensosi dibatti in merito alla possibilità per il mezzo televisivo di influenzare le scelte politiche dei cittadini.

Penso che questi dibattiti siano poi stati superati dalla storia, e adesso spero possiamo evitare di rifare lo stesso errore con i *social network*, perché mi sembra evidente che i *social network* ci possano influenzare, dobbiamo solo chiederci quanto.

Il fatto che ci sia la possibilità di fare influenza tramite i *social network*, di spostare il comportamento della nostra società e della politica non è irrilevante, per due motivi.

Il primo è che, se osserviamo la *slide* con tutte queste minacce, man mano che ci siamo spostati da una cosa all'altra, abbiamo ampliato lo spettro delle competenze che servono per fare *cybersecurity* nazionale.

Siamo partiti dalla *cybersecurity* che si fa con i *backup* e con gli *antivirus*, siamo passati a doverci chiedere “Questa aggressione è una cosa strategica? Chi c’è dietro? Con che scopo?”.

Poi siamo passati a parlare di aggressioni massicce portate da organismi statali (e sappiamo che non è certo solo la NSA a farlo, anzi, tutti gli Stati di una certa dimensione e importanza si sono attrezzati in questo modo, ad esempio con i gruppi chiamati APT, *Advanced Persistent Threat*).

Infine siamo arrivati ai *social network* dove, anche soltanto per capire quale sia l’impatto, abbiamo bisogno anche delle competenze di sociologi, massmediologi, politologi.

Voi capite che l’orizzonte di chi si occupa di *cybersecurity* oggi è estremamente ampio.

Nessuno ha tutte le competenze che servono per fare *cybersecurity* oggi, perché è un campo interdisciplinare che va dall’ingegneria alla giurisprudenza, dalle scienze politiche a quelle sociali, fino ad arrivare a campi come l’analisi degli equilibri internazionali. Persino tra gli informatici che si occupano degli argomenti più tecnici ci sono varie specializzazioni.

Io mi occupo di analizzare *malware* e di capire come faranno gli aggressori ad attaccare le automobili iperconnesse del nostro futuro, e colleghi che fanno il mio stesso lavoro, che hanno la stessa estrazione, allo stesso modo si sono specializzati nell’analizzare gli impatti sui *social network*, come l’amico Gianluca Stringhini di Boston University.

Io posso capire il suo lavoro, ma facciamo sostanzialmente due lavori diversi, anche se entrambi facciamo *cybersecurity*.



<http://gizmodo.com/385113>this-is-how-cyber-criminals-party-menus-and-blow-up-dolls>

Lasciando a Gabriele Faggioli l'analisi di dati sul mondo del *cybercrime*, mi limito ad un'osservazione relativa al grande universo dei criminali finanziariamente motivati.

Questa è un'immagine che mi piace sempre far vedere, perché i signori che ci sono in questa immagine, oscurata in ossequio al fatto che siamo presso l'Autorità Garante per la protezione dei dati personali, ma che nella sua versione originale non è oscurata, sono membri di una *gang* di *cyber* criminali.

La valigetta è piena di banconote da 50 euro. La cosa che trovo però personalmente irresistibile di questa immagine è il fatto che questi signori hanno al collo un *badge*, perché questa è una conferenza *business* per *cyber* criminali. In molte regioni questo tipo di crimine o non è previsto dalla legge locale, oppure non è banalmente punito perché non c'è l'*enforcement*.

Essendo un crimine transnazionale, sappiamo che gli sforzi per contenerlo sono difficili e limitati.

Di buono c'è che questi aggressori, finanziariamente motivati, rendono semplice la valutazione delle tecniche di difesa. Ci basta far sì che il loro attacco costi più di quello che guadagnano per renderli inoffensivi o incoraggiarli a cambiare bersaglio.

Per questo, nelle *slide* precedenti, gli aggressori più difficili

da gestire sono quelli non finanziariamente motivati: Stati, gruppi non statali di terroristi o di organizzazioni che sono motivate da altro.

Queste organizzazioni sono più difficili da scoraggiare, ed è lì che si genera il tema della *cybersecurity* nazionale, una *cybersecurity* che, siccome trascende il *budget* dei singoli cittadini o imprese nel difendersi, ha bisogno dell'intervento regolatorio ma anche economico e di mezzi dello Stato.

Quello è il terreno dove come cittadini, nel contesto del nostro patto sociale, abbiamo necessità di una difesa comune: esattamente come abbiamo le forze dell'ordine e le forze armate, che mettono insieme il *pool* di risorse e di competenze che servono per difenderci su quei terreni dove come singoli cittadini non ci possiamo difendere e non ha senso che ci difendiamo; allo stesso modo c'è una parte di protezione informatica che è nostro dovere personale, ma c'è anche una parte di *cybersecurity* che è necessariamente compito delegato allo Stato.

Riguardo alla capacità di difendersi da parte delle imprese, l'Italia ha varie peculiarità rispetto ad altri Paesi.

La più importante è che le imprese italiane sono in grandissima parte piccole e medie, ma tra queste vi sono dei veri gioielli, che hanno delle quote di *leadership* di mercato in un loro specifico settore di nicchia di proporzioni epiche.

Tutte queste aziende hanno un problema significativo: hanno un *asset* che ha valore e, dall'altra parte, non hanno necessariamente né le competenze né la possibilità di acquisirle in maniera economicamente sensata per proteggere questo *asset*.

Su questa difficoltà deve intervenire lo Stato, e anche il sistema Confindustriale; e serve che lo si faccia ora, anche perché tutti i dati ci dicono che la dimensione di una azienda "significativa a sufficienza" da essere soggetta ad attacchi *targeted* (in altre parole, la barra di quando diventi interessante al punto tale che qualcuno non è che attacca te come chiunque altro, ma proprio perché sei tu) continua a scendere. Le aziende italiane inoltre,

anche grazie al meritorio piano Industria 4.0, si stanno mettendo in rete.

Questo è fondamentale per la loro competitività, ma proprio al mio gruppo al Politecnico siamo stati tra i primi al mondo a delineare le vulnerabilità di questo tipo di sistemi (trovate le nostre ricerche sulla protezione delle fabbriche intelligenti al sito <http://robosec.org>, anche con dei video).

# Sicurezza informatica: i nuovi dati

## Clusit e Osservatorio Cybersecurity & Data Protection Politecnico di Milano

**Gabriele Faggioli**  
*Presidente del Clusit*  
*Adjunct Professor MIP-Politecnico di Milano*

---

Per chi non lo sapesse, il Clusit è la più grossa Associazione italiana che si occupa di sicurezza informatica. Tra l'altro in questi giorni ricorrono i vent'anni dalla fondazione, fra un mese e mezzo faremo il *security summit* a Milano<sup>(1)</sup>, i tre giorni in cui tutti gli anni noi presentiamo il nostro rapporto<sup>(2)</sup> e poi lo rinnoviamo con cadenza semestrale. Quest'anno, per la prima volta, proprio per l'invito che ci è stato fatto, abbiamo deciso oggi di presentarvi qualche dato in anteprima, che presenteremo in modo completo fra un mese e mezzo.

Per chi non conoscesse *l'Osservatorio information security & privacy*<sup>(3)</sup> può essere utile sapere che in seno a Ingegneria gestionale a Milano è stato creato oltre venti anni fa l'iniziativa di ricerca denominata *Osservatori della Digital Innovation* con l'obiettivo di fare cultura in tutti i principali ambiti di Innovazione Digitale.

Il Rapporto del Clusit e la ricerca dell'Osservatorio hanno obiettivi diversi. Il Rapporto del Clusit va molto sul fenomeno, quindi vedrete dei dati legati alle tipologie di attacchi e a quelli che sono i *target* tipicamente, invece lo studio dell'Osservatorio

---

(1) Rimandato all'autunno a causa dell'emergenza Covid-19.

(2) Presentato in video con anche la partecipazione del dott. Giuseppe Busia.

(3) Il nome è stato modificato successivamente in *Osservatorio Cybersecurity & Data Protection*.

del Politecnico - e oggi vi presenterò in anteprima qualche dato che presenteremo il 5 febbraio a Milano - analizza un po' più il tema del mercato, quindi come le aziende e le pubbliche amministrazioni investono, si organizzano e affrontano la tematica.

Le due ricerche hanno quindi due tagli diversi, e oggi vi darò un po' di dati in anteprima tratti da entrambe. Io ho visto tutti i casi che sono stati raccontati, però vi racconto un piccolo caso completamente diverso da quelli che hanno raccontato gli altri relatori, che mi piace raccontare perché dà l'idea che il tema della sicurezza della protezione del dato e della sicurezza informatica sta molto aumentando.

Prima sono stati ringraziati i giornalisti e l'attenzione mediatica sul tema *cybersecurity* dà l'idea della importanza del tema al giorno d'oggi. Qualche settimana fa mi ha telefonato una giornalista di una rivista non certo nota per essere specializzata in sicurezza informatica, "Famiglia Cristiana", che intuitivamente tratta altri tipicamente altre tematiche, e l'oggetto dell'intervista era se l'utilizzo dei POS per i pagamenti tramite carta di credito nelle chiese per raccogliere l'obolo dei fedeli pone dei problemi di sicurezza o meno.

Il tema è interessante, perché ovviamente parliamo di vita quotidiana, siamo lontanissimi da un'infrastruttura critica, siamo lontanissimi dalle macchine interconnesse, però vuol dire che una giornalista si è posta il problema che avere il POS con la carta di credito che magari do in mano al chierichetto che gira per la chiesa qualche problema lo potrebbe porre.

Quel caso mi ha fatto pensare che effettivamente è cambiato molto.

Chi veniva ai nostri lavori al Politecnico cinque o sei anni fa, veniva da addetto ai lavori e tipicamente ci chiedeva "come faccio a farmi dare il *budget*".

Come faccio a farmi riconoscere e dimostrare la mia esistenza in azienda".

Oggi è diverso - vedremo anche qualche dato -, i CISO esistono eccome, i presidi interni di sicurezza esistono eccome, le funzioni di *privacy* esistono. Certo con larghissimi margini di miglioramento (vedrete poi una *slide* che temo diventerà il piano semestrale dei controlli del Garante 2020...).

Insomma, il tema ormai è sicuramente molto maturato.

Questo non vuol dire che sia completamente maturo, non vuol dire che siamo arrivati, assolutamente, però qualche elemento di positività è anche giusto a mio avviso darlo.

Gli attaccanti (2019 - 10 mesi)							
ATTACCANTI	2017	2018	2019*	2017%	2018%	2019*%	Totale
Cybercrime	857	1232	1140	76%	79%	83%	3229
Espionage / Sabotage	79	61	164	7%	4%	12%	304
Hacktivism	129	203	35	11%	13%	3%	367
Information warfare	62	56	30	6%	4%	2%	148
<b>TOTALE</b>	<b>1127</b>	<b>1552</b>	<b>1369</b>				<b>4048</b>

• L'analisi comprende un campione complessivo di 4.048 attacchi.

• Gli attacchi sono in prevalenza di natura Cybercrime (80% del totale).

• Le tecniche più utilizzate nel periodo sono Malware (40%) e Unknown / Data breach (24%).

Questo è il primo dato. Innanzitutto un chiarimento. Quando parliamo della ricerca del Clusit per il 2019, in questo momento, parliamo di dieci mesi, perché al momento sono riuscito a farmi dare dai miei colleghi, che ringrazio per il lavoro che fanno al Clusit, i dati su dieci mesi di analisi.

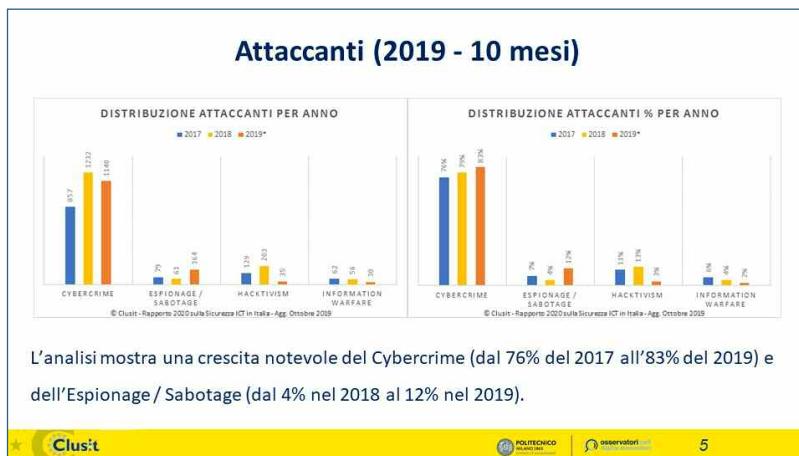
Ritengo che il dato interessante sia la seconda riga: l'incredibile aumento delle casistiche di spionaggio e sabotaggio.

Questo non mi sorprende.

Quando Stefano ha detto prima - e concordo pienamente - che si fanno gli attacchi per diversi motivi, ma ce n'è uno più importante degli altri, i soldi, quello mi dice tutto (è infatti evidente che le casistiche di *activism* sono crollate).

Tenete conto che noi come Clusit accediamo a informazioni che sono pubbliche, non abbiamo informazioni riservate, semplicemente ne aggreghiamo tante, quindi pensiamo di riuscire ad inquadrare il fenomeno; dentro questi numeri voi vedete quelli che noi classifichiamo come attacchi “critici”, di alta rilevanza in termini di gravità.

Sono ovviamente di più quelli che accadono veramente, i numeri che vi presento sono quelli che noi conosciamo inerenti gli attacchi ad alta severità. L'attenzione da questo punto di vista a mio avviso va posta sui casi di spionaggio e sabotaggio. Notate anche (ultima riga) la discesa costante in questi anni di aspetti di *information warfare* che noi colleghiamo a quella che è stata due o tre anni fa la situazione dell'Isis, e a tutto quello che si è portato dietro in termini di tensioni internazionali.



Nella seconda *slide* vedete gli stessi numeri spaccati in una distribuzione percentuale numerica.

Molto interessanti in questa vista le casistiche di *cybercrime*: dal 76 all'83 per cento. In pratica, il *cybercrime* la fa enormemente da padrona come numeri, questo da sempre.

La motivazione io la collogo al fatto che sono tantissimi attacchi, se volete anche meno onerosi da fare, meno costosi,

più semplici che mirano ad attaccare un numero molto ampio di soggetti *target*.

Oggi non vi ho portato nelle *slide*, perché non l'abbiamo ancora elaborata, ma ci sarà a marzo, la valutazione dell'impatto delle singole tipologie di attacco. Ecco, mentre i casi di *cybercrime* tipicamente hanno un impatto un pochino più basso, se prendo un singolo caso, l'impatto medio dei casi di spionaggio e sabotaggio invece, quando riescono, è estremamente elevato.



Questa è invece la distribuzione dei *target*, cioè dei soggetti attaccati. Vedete che sono numeri molto importanti quelli degli attacchi multipli. Notate anche la seconda categoria su cui poi farò uno zoom: l'attacco ad enti governativi, militari, *law enforcement* e *intelligence*.

Mi fermerei un momento però sul quarto, che ritengo sia un dato importante: quello legato ai servizi *on line* e *cloud*.

È evidente che noi siamo in un mondo dove c'è una fortissima spinta all'esternalizzazione, questo sia nel mondo pubblico che nel mondo privato; noi abbiamo anche degli studi che facciamo su questo tema, ed io ho avuto la fortuna di lavorare con la Commissione europea sulla politica di sviluppo del *cloud computing* in Europa.

Ritengo che questa spinta verso l'esternalizzazione e il *cloud* sia un percorso in questo momento ineludibile, in qualche modo dovuto sia per motivi di efficienza tecnologica e di aggiornamento, ma io lo vedo anche sotto il profilo della sicurezza.

Il poter accentrare le infrastrutture, le applicazioni e i dati può avere vantaggi e svantaggi a seconda dei punti di vista. Ma io ritengo i vantaggi maggiori, ritengo che le capacità di investimento che possono mettere a terra i grandi *player* dei servizi *cloud* sono del tutto impossibili per le aziende più piccole che non potranno mai stare dietro all'innovazione e alle esigenze di sicurezza.

D'altronde io presumo che molti di voi i soldi o i gioielli li mettano nelle cassette di sicurezza delle banche piuttosto che sul conto corrente, e non si fanno invece un mini *caveau* in casa propria. Per ovvi motivi.

Questo è il percorso e in questa direzione, non certo assoluta e per carità, si continuerà ad andare.

Possiamo essere d'accordo o meno sul fatto che il *cloud* possa essere più o meno sicuro o possa proporre problemi sul trattamento dei dati, però è un dato di fatto che il mercato sta andando lì.

Quindi, per quanto possiamo anche provare a mettere dei freni, in realtà la domanda è se poi l'apparato normativo e quelle che sono le scelte che si fanno sono adeguate a proteggere le informazioni per permettere di andare in una direzione di tranquillità verso questi servizi. Però non possiamo non evidenziare che naturalmente questo sarà un settore che sarà sempre più obiettivo di attacchi, perché naturalmente sfondare sistemi in *cloud* dove ci sono dati di centinaia di milioni o miliardi di soggetti, evidentemente, fa gola a molti.

L'altro dato che vi faccio notare è quello della terza categoria: il mondo sanitario. Il mondo sanitario è tipicamente un mondo fortemente attaccato, tipicamente da attacchi di *cybercrime*, tipicamente da attacchi di *malware*, perché l'esigenza

di sbloccare l'utilizzo del dato conseguente al blocco che mi deriva dal *malware* è fondamentale per procedere nelle cure.

Ritengo, che un ospedale non possa permettersi di bloccare le cure e, quindi, sono tipicamente target considerati a più facilità di ottenimento di denaro una volta che l'attacco dovesse andare a buon fine.

Il fatto stesso che ci siano gli attacchi e che vadano a buon fine, come peraltro i giornali, non solo nel mondo ma anche in Italia, hanno riportato negli ultimi mesi, denota il fatto che c'è ancora una immaturità sotto il profilo della prevenzione, peraltro probabilmente anche in violazione delle norme.

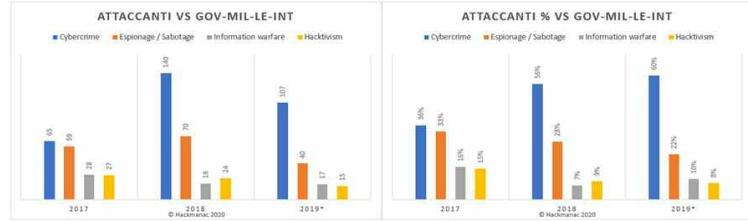
Passerei ora a illustrare un *focus* che abbiamo preparato per questo evento e che troverete nel rapporto, legato verticalmente al tema delle infrastrutture critiche, al tema del settore governativo militare, *law enforcement* e *intelligence*, e poi al tema della filiera di questo ambito.

Quindi *contractor* e *consulting* all'interno del mondo pubblico e privato, quando struttura critica.



Qui vedete un po' i numeri percentuali che riprendono e spaccano i numeri che abbiamo visto prima.

## Attaccanti vs GOV – MIL – LE – INT



Sebbene in termini numerici assoluti la distribuzione mostri apparentemente una decrescita, l'analisi percentuale evidenzia invece una crescita degli attacchi dovuti a Cybercrime diretti ad enti governativi (passati dal 36% nel 2017 al 60% nel 2019).

Clusit

POLITECNICO  
di MILANO

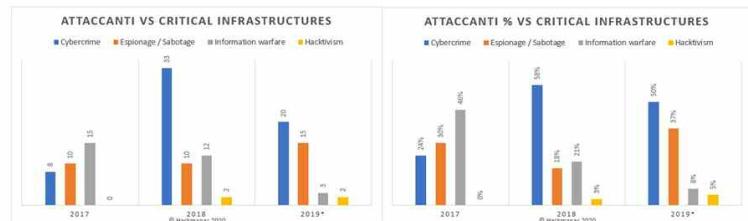
Osservatorio

10

Mi interessa però farvi vedere alcuni dati un pochino più puntuali. Qui entriamo nel merito degli attaccanti contro il mondo governativo e militare: c'è in qualche modo una diminuzione del valore assoluto numero (poi vedremo i dati di fine anno), notate però che c'è un'esplosione in due anni, dal 36 al 60 per cento, degli attacchi dovuti al *cybercrime*.

Questi dati secondo noi sono utili, perché danno una chiave di lettura del fenomeno e - fatemi dire - è anche l'evidenza della necessità di aumentare o comunque orientare gli investimenti in particolare in relazione ai sistemi di protezione dalle minacce più evidenti o comunque potenzialmente più dannose.

## Attaccanti vs critical infrastructures



Mentre sembrano diminuire gli attacchi dovuti a Cybercrime e Information warfare, l'Espionage / Sabotage verso Infrastrutture Critiche è in forte crescita (dal 24% nel 2017 al 37% nel 2019).

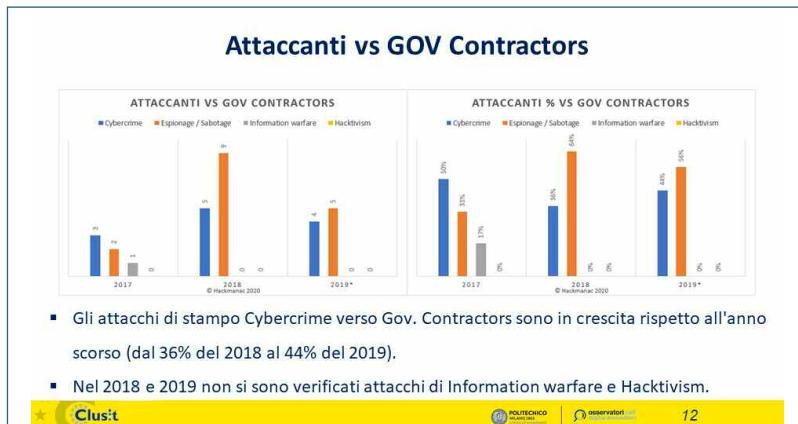
Clusit

POLITECNICO  
di MILANO

Osservatorio

11

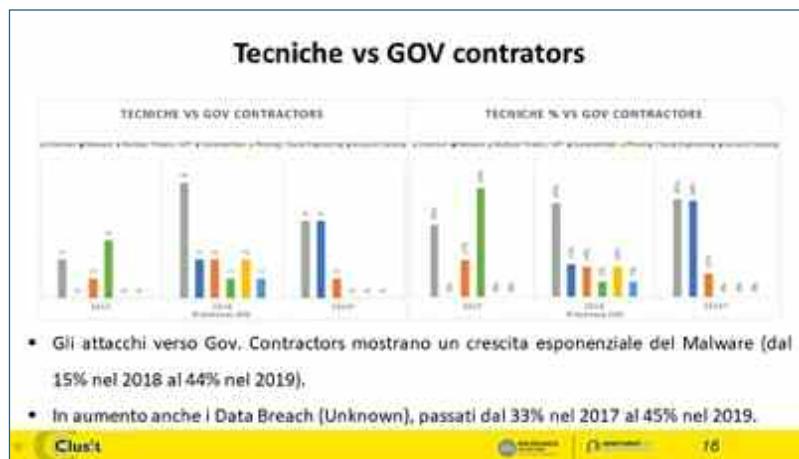
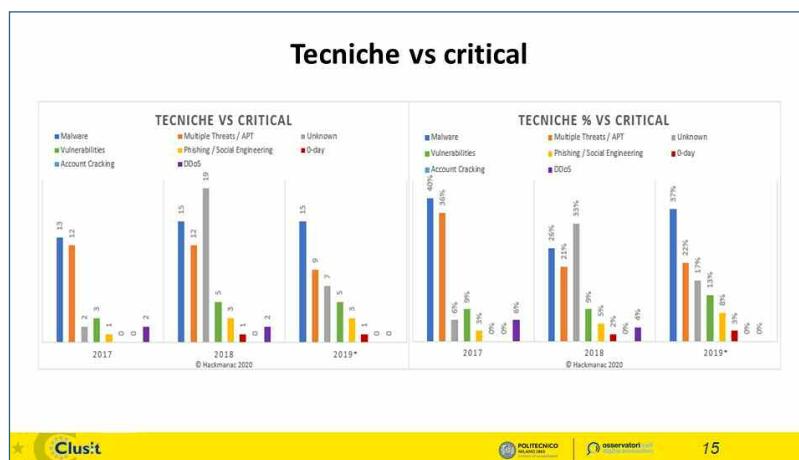
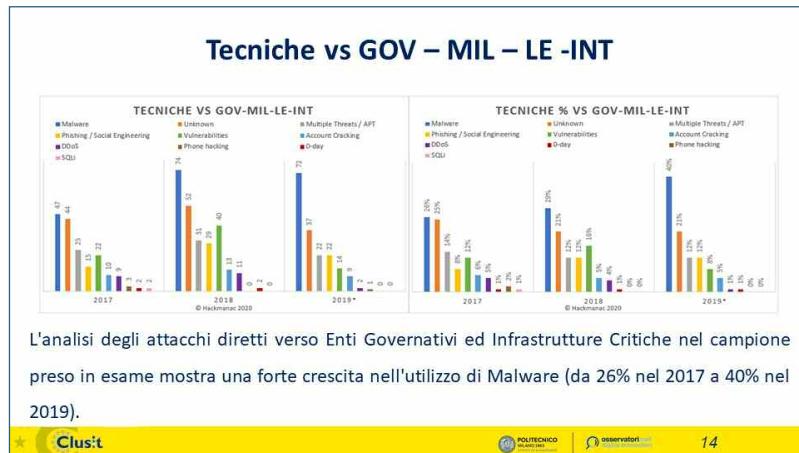
Sull'aspetto invece degli "attaccanti" le infrastrutture critiche notate, soprattutto tra il 2018 e il 2019, il salto delle casistiche (la sbarra arancione) del tema dello spionaggio. Quindi c'è proprio uno spostamento dall'*hacktivism* allo spionaggio e sabotaggio (se volete anche un po' uno svuotamento dell'*hacktivism* come evidente analizzando la linea grigia) come si evidenzia dal fatto che il tema dello spionaggio e del sabotaggio verso le strutture critiche comincia ad essere una percentuale che preoccupa per la numerosità dei casi gravi che si vanno a mappare.

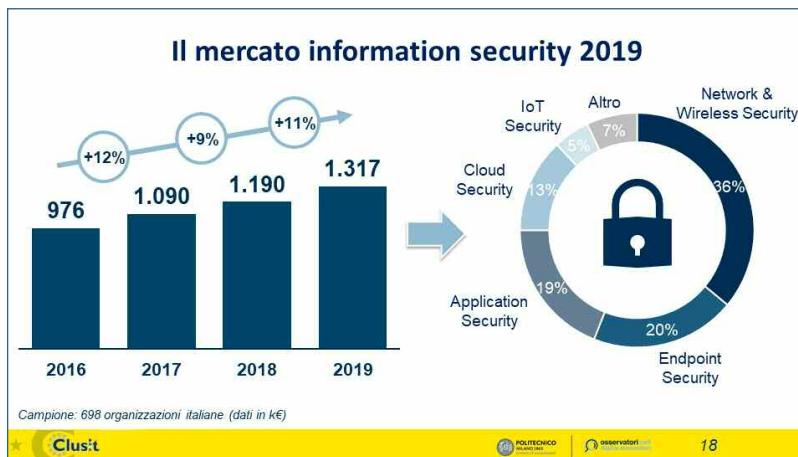


Verso i *contractor* questo fenomeno è ancora più evidente. Qui parliamo della filiera dei fornitori e vedete come in valore assoluto sono pochi numeri, sono pochi casi, però la maggior parte (siamo al 56 per cento, 64 l'anno scorso) è fortemente legata a spionaggio e sabotaggio, che non è strano. Devo dire che anche le scelte del *Cybersecurity Act* vanno in una direzione giusta secondo noi, ottima come scelta normativa il proteggere non solamente le strutture in quanto tali ma tutto il perimetro della filiera.

L'ultima *slide* e poi passo ai dati del Politecnico, mostrano le tecniche di attacco. In realtà poi nelle slide ci sono anche le altre categorie, vi faccio vedere solo questa per motivi di tempo.

Vedete che la sbarra blu, che riguarda il *malware*, la fa da padrona. Ma i dati degli impatti effettivi dei casi sono un pochino più limitati.





Passiamo ora ad analizzare qualche dato preso dalla ricerca del Politecnico.

Il 5 febbraio le esporremo nella loro interezza.

Intanto il mercato. Noi siamo il Politecnico di Milano, abbiamo una ricerca fatta su quasi settecento organizzazioni, di cui centottanta di grandi dimensioni, quindi i numeri che diamo sono numeri per cui cerchiamo di arrivare a qualcosa di più preciso possibile senza possibilità però di avere una analisi di tutto il mercato. In genere, comunque, riteniamo di stimare correttamente l'ordine di gradezza dei numeri che presentiamo.

Vedete che in relazione agli investimenti dal 2016 ad oggi c'è un salto importante, perché parliamo di poco meno del 50% di crescita in termini di spesa.

Questa spesa soprattutto nei primi due anni è stata fortemente dettata dal GDPR e dalla spesa che le pubbliche amministrazioni e le società private hanno messo in campo per poter far fronte all'impatto normativo; da una ricerca di quest'anno emerge anche un aumento della spesa dovuta anche alla maturità raggiunta nelle imprese perlomeno di grandi dimensioni in relazione ai rischi *cyber*. Poi questa è una spesa che si spacca in tante tipologie di ambiti. E poi c'è tutto un tema ancora legato alla *compliance* molto importante.

## Qual è il trend degli investimenti in sicurezza informatica



Il mercato dell'information security cresce di circa l'11% e si attesta a 1.3 miliardi di euro

Il 51% delle grandi aziende ha dichiarato di aver aumentato il budget a fronte del solo 2% che ha dichiarato di averlo ridotto

Per la protezione delle risorse in cloud il 55% delle grandi aziende ha dichiarato di aver aumentato il budget

Fonte: Osservatorio Information Security & Privacy Politecnico Milano – Ricerca 2020



19

Vi faccio notare due numeri che non trovate in questa *slide*, ma poi nella ricerca sono esplosi.

Il 51 per cento delle grandi aziende ha dichiarato di aver aumentato il *budget* in sicurezza e solo il 2 per cento di averlo diminuito, ma il terzo dato che vi cito, e che mi riporta sul tema del *cloud* e dell'esternalizzazione, è che il 55 per cento delle grandi aziende ha dichiarato di aver aumentato la spesa sulla sicurezza per il *cloud*. Questo significa che oggettivamente quello è un ambito, una direzione in questo momento ancora molto importante.

## Le scelte organizzative



Nel 40% delle organizzazioni non esiste una specifica funzione Information Security (dato ancora fortemente negativo)

Oltre la metà delle organizzazioni ritiene che il modello organizzativo adottato non rappresenti una configurazione ottimale per un'efficace gestione dell'information security

In particolare, il grado di insoddisfazione raggiunge un picco del 65% tra le aziende in cui la funzione Information Security riporta all'IT

Il 90% delle organizzazioni che hanno adottato il modello nel quale il CISO è a riporto del Board ritiene che tale configurazione sia ottimale

Fonte: Osservatorio Information Security & Privacy Politecnico Milano – Ricerca 2020



20

C'è poi tutto il tema delle scelte organizzative, e non solo di quelle tecnologiche. C'è un 40 per cento di imprese intervistate che non ha una funzione di *information security*. Questo è un dato fortemente negativo anche se, leggendolo nella prospettiva degli ultimi anni, il dato sta migliorando pur essendo ancora basso. Vi faccio notare il terzo e il quarto punto. Qui sarebbe interessante sapere quante aziende hanno il CISO a riporto del *board*, perché è emerso che il 90 per cento delle aziende intervistate lo hanno ritenuto essere il modello ideale mentre oggi molte realtà hanno ancora l'*information security* che riporta all'*IT manager*, al CIO, e questo non è considerato performante da un punto di vista organizzativo.

### Il fattore umano

Nel 55% dei casi, esiste un piano di formazione pluriennale, che coinvolge tutta l'organizzazione, dal Top Management alle Business Line.

Nel 25% del campione vi è un piano di formazione indirizzato nello specifico a funzioni con maggiore sensibilità alle tematiche di information security e data protection, quali IT, Risk Management e Compliance

Il 20% delle aziende gestisce le iniziative di formazione in modo spot, senza un piano strutturato

Clusit 21

### Di cosa hanno paura le aziende nel mondo industriale (Industry 4.0)

Fermo parziale o totale della produzione (54%), che può sia costituire l'obiettivo diretto e primario di un eventuale attacco sia rappresentare invece una ripercussione secondaria

Tra le conseguenze più rilevanti si trova poi la safety (20%), requisito reso particolarmente critico dall'interazione sempre più diretta tra operatori e macchine (es. robotica collaborativa)

Possibile alterazione o modifica della produzione (16%), con motivazioni riconducibili al sabotaggio

È invece considerata meno rilevante in questo ambito la possibilità di furto, perdita o divulgazione di dati confidenziali (10%), principalmente riguardanti la proprietà intellettuale.

Clusit 22

Il fattore umano, spesso considerato l'anello debole della catena come si usa dire, e concordo, è ancora tema di grande rilevanza.

Notate però che su centottanta grandi aziende intervistate il 50 per cento ha un piano di formazione sui temi di *privacy* e *security* strutturato e pluriennale, che coinvolge peraltro il *top management*, e questo è un altro elemento di maturità; un 25 per cento ha dei piani di formazione verticali, però strutturati sull'anno; poi c'è un 20 per cento, che però è tutto sommato andato basso - e questo ci conforta - che invece ancora va un po' alla cieca.



Intelligenza artificiale. C'è un grosso dibattito se l'intelligenza artificiale sarà più utile per contrastare il fenomeno *cyber* o se invece sarà più utile come strumento di attacco, e questo lo vedremo nei prossimi anni.

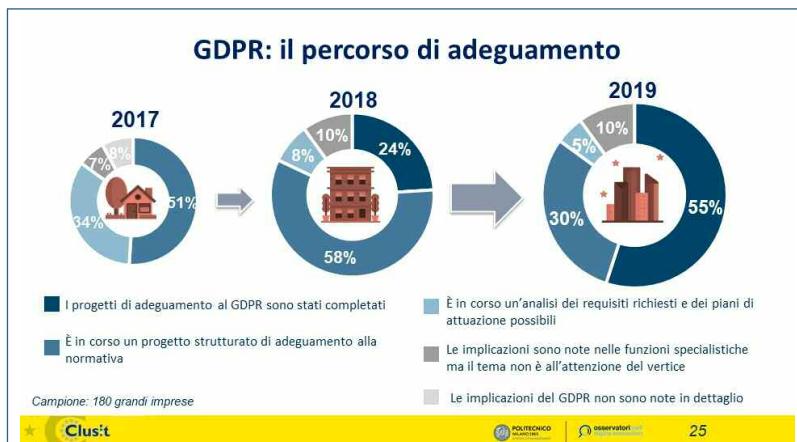
Centottanta grandi imprese, il 45 per cento del campione, ha però dichiarato che già ora usa sistemi di intelligenza artificiale a protezione dei dati e della propria sicurezza interna.

Comincia a essere un numero importante.

Naturalmente sono sistemi di intelligenza artificiale molto orientati ad alcune tipologie di attività, in particolare

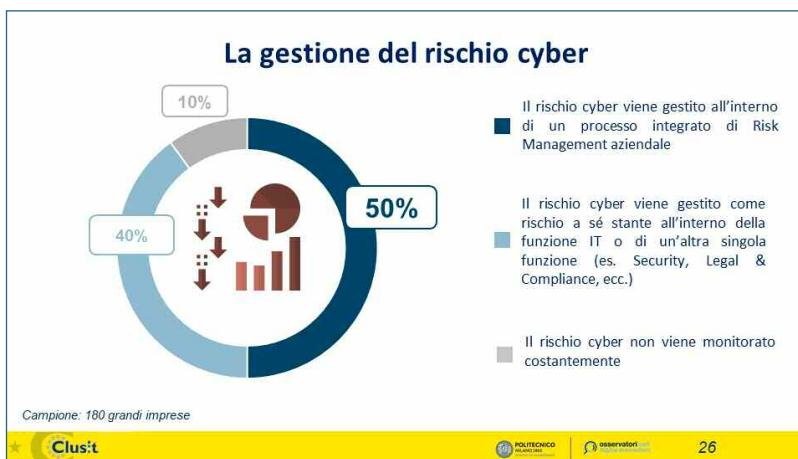
tutto quello che vuol dire correlazione di eventi e *detection* di anomalie, identificazione minacce e vulnerabilità “zero day”.

Però parliamo comunque di prodotti e servizi sul mercato che cominciano ad avere una diffusione importante, su cui sarà interessante vedere cosa prevarrà tra chi li usa per attaccare e chi per difendersi.



Questa è invece la *slide* che, facendo una battuta, può rappresentare il piano di visite semestrali dei controlli dell'Autorità.

Lo dico perché i dati sono molto positivi sullo stato di adeguamento al GDPR, meno positivo che c'è un 15 per cento di grandi imprese (ventisette su centottanta, quindi non pochissime) che hanno dichiarato di non aver ancora affrontato il tema GDPR in modo strutturato e che le implicazioni sono note nelle funzioni specialistiche ma il tema non è all'attenzione del vertice. Può anche darsi che gli intervistati non fossero pienamente a conoscenza del tema, quindi mi riservo su questo, però, se vedete, il 30 e il 55 per cento invece hanno dato delle indicazioni di adeguamento molto spinto.



L'ultima *slide* e poi mi fermo sui numeri, poi, se avete qualche approfondimento o curiosità, volentieri: la gestione del rischio *cyber*. Un 50 per cento di aziende, qui siamo sempre nelle centottanta delle aziende grandi, quindi non mi sorprende dato, il rischio *cyber* viene gestito all'interno di un processo integrato di *risk management* aziendale.

Quindi c'è una gestione strutturata del tema. Un 40 per cento dichiara che viene gestito come rischio a sé stante in ambito IT o altre funzioni, però almeno è percepito. Il 10 per cento di fatto non considera il tema di particolare rilevanza.

Due considerazioni finali.

Da una parte siamo davanti sicuramente a un fenomeno ancora in grosso aumento, e continuerà ad aumentare. D'altronde, prima si è parlato di superficie d'attacco: se la superficie d'attacco aumenta, aumentano anche gli attacchi. C'è poco da fare. Quindi non arretrerà mai questo fenomeno.

Noi abbiamo, sia come Politecnico che come Clusit, la percezione che nello strato alto delle aziende italiane, per dimensione o per tipo di *business*, cominciano ad essere temi affrontati. Anche a livello occupazionale devo dire si è fatto tantissimo.

Se guardate anche gli indicatori sul mercato del lavoro di chi si occupa di *security* e *compliance*, è un mercato estremamente attivo in questo momento. Stefano è più di me testimone dell'alleanza tra il Politecnico e la Bocconi su un percorso formativo verticale su queste tematiche.

Il mercato del lavoro sta cercando risorse. Chi si mette in questo mercato, se avete figli che vogliono entrare nel mercato del lavoro, questo è un settore in cui trovano lavoro immediatamente. Quindi a livello occupazionale, di investimenti e di tecnologie, si sta facendo molto.

Certo, la sfida è continua, perché l'aspetto degli attacchi è talmente in evoluzione che non avremo mai il momento finale di questa battaglia.

Un dato, che non ho ancora ma che sarà nel rapporto, è la numerosità dei casi di *data breach* e anche di attacchi per zona geografica del mondo. Fino all'anno scorso, se guardate il rapporto Clusit per il 2018 - adesso vedrete quello del 2019 - la faceva da padrona il Nord America e l'Europa aveva una fettina molto piccola. Veramente una percentuale molto bassa di casi. L'Italia è una fettina minuscola.

Io ho sempre pensato che quel dato derivasse dal fatto che le zone del mondo tecnologicamente più avanzate fossero anche più esposte, anche più ricche, quindi in qualche modo più appetibili ma, in realtà, i miei colleghi al Clusit mi dicono

che sbaglio e che il motivo è un altro: in Europa e in Italia, senza le normative che costringono a segnalare le violazioni, c'è omertà e a nessuno fa piacere dichiararlo, quindi o la notizia esce per qualche motivo o non si sa, quindi è ovvio che i numeri siano più bassi. Vedremo quest'anno cosa emergerà, visto che adesso invece le segnalazioni si fanno e i casi naturalmente arrivano alla nostra conoscenza.

Oggi molte normative impongono la comunicazione dei casi alle Autorità competenti e in taluni casi ai soggetti che hanno subito le violazioni e quindi è naturale che si conoscano più casi. Non mi sorprende però, intanto perché il fatto che ci sia più attenzione non vuol dire assolutamente che non capitino casi. Il fatto che ci sia un maggior investimento non vuol dire che si evitino o si respingano tutti i possibili attacchi che ci possono essere. Esistono poi tantissime casistiche dove l'attacco non arriva dall'esterno ma è dall'interno: personale infedele, persone che cambiano azienda e si portano via informazioni, che se le vendono.

Sono casi estremamente difficili da evitare o scoprire. Io posso avere tecnologia, posso avere procedure, posso avere tanto, ma, se qualcuno mi vuole fare un attacco, i suoi mezzi possono essere migliori dei miei, può avere maggiore capacità, può essere semplice effettuare un attacco.

Poi c'è il problema di poter adottare misure adeguate per tutti gli attacchi potenziali, che è impossibile anche solo per motivi di costo.

È chiaro che le statistiche anche sul tempo in cui certi *data breach* vengono scoperti, che è un numero di giorni incredibile (oltre duecento il dato che avevo), è estremamente preoccupante, però non ci può sorprendere.

Ci sono casi che oggettivamente, anche dal punto di vista della capacità dell'attaccante, magari dall'interno, di fare azioni malevoli è oggettivamente difficile da intercettare.

Ci può essere solo una parola, ci può essere un caso, quello

di Unicredit, dei grandi *data breach* che è preoccupante, per fortuna su pochissimi *set* di dati, ma il caso che io faccio sempre del non *data breach*, ma che poteva essere molto importante, è quello di Sergio Marchionne. Della malattia che poi lo ha portato alla morte si è saputo pochissimi giorni prima, ma quando hanno dichiarato che lui si curava da un anno a Ginevra, qualcuno là lo sapeva, e la capacità di tenere segreta una notizia, una, solo quella, dell'amministratore delegato di una delle più importanti aziende italiane, e anche nel mondo, malattia mortale che ha portato a un crollo del titolo dell'11 per cento il giorno della morte, rende chiaro il valore di quell'informazione.

Quindi il problema non è solo nei tre, trenta o trecento milioni di interessati coinvolti, ci sono anche casistiche che possono essere molto più piccole, molto più puntuali ma con degli impatti molto più violenti.



GARANTE  
PER LA PROTEZIONE  
DEI DATI PERSONALI

Redazione  
Garante per la protezione dei dati personali

Piazza Venezia, 11  
00187 Roma  
tel. 06 69677.1  
[www.garanteprivacy.it](http://www.garanteprivacy.it)  
e-mail: [protocollo@gpdp.it](mailto:protocollo@gpdp.it)

A cura del  
Servizio relazioni esterne e media

Stampa:  
Tiburtini s.r.l.