GIGI TAGLIAPIETRA*

La protezione dell'intangibile

1. *La smaterializzazione del valore*

Uno degli effetti indotti dallo sviluppo delle tecnologie della comunicazione è il progressivo trasferimento di valore dai beni tangibili a quelli immateriali. Tutti abbiamo visto anche gli effetti clamorosi nelle valutazioni economiche delle prime aziende quotate in borsa della cosiddetta 'New Economy'.

Nonostante lo scoppio della bolla speculativa, il processo di smaterializzazione è proseguito e il valore dei patrimoni intangibili nelle aziende, per quanto difficile da misurare oggettivamente, è lì a spiegarci la differenza tra le valutazioni di bilancio e i prezzi pagati per aziende come Skype o YouTube.

Il processo non riguarda solo i fattori economici legati al mondo dell'impresa, ma anche la nostra sfera personale in cui da un'economia di possesso di beni stiamo passando a una basata invece sull'utilizzo di servizi. Avendo risolto i bisogni primari di sussistenza e sopravvivenza, crescono poi le nostre aspettative circa la 'qualità della vita': un valore difficile da misurare, ma che diventa fonte di motivazione sempre più determinante per scelte importanti che ci riguardano.

Se dalla cultura dei castelli, dei forzieri, dei catenacci e degli eserciti abbiamo imparato come difendere i beni materiali, come proteggiamo i beni intangibili? Si tratta innanzitutto di riconoscerne il valore. Nella vita di tutti i giorni compiamo azioni riconducibili al tema della sicurezza: chiudiamo la porta di casa, ci fermiamo ai semafori, diamo da mangiare ai nostri figli. Solitamente agiamo con discernimento trovando il giusto equilibrio tra l'azione che compiamo e il risultato che intendiamo ottenere perché

* Presidente CLUSIT, Associazione Italiana per la Sicurezza Informatica.

abbiamo in mente una precisa scala di valori, valida spesso solo per noi, ma pur sempre un preciso riferimento: proteggiamo ciò cui attribuiamo un valore.

Quando ci troviamo di fronte a problemi di sicurezza delle informazioni, la prima domanda che ci dobbiamo porre è: quale valore viene dato alle informazioni?

Trascurando il fatto se le informazioni in quello specifico contesto abbiano un oggettivo valore alto o basso, dobbiamo chiedere quale sia il loro valore percepito dai soggetti.

L'esperienza insegna che a nulla valgono le soluzioni (anche sofisticate) che non si basino su una precisa definizione e condivisione del valore dell'informazione da proteggere e della criticità della infrastruttura che la deve rendere affidabile e fruibile. E questo, tanto nel mondo delle aziende che nella sfera personale.

Oggi parliamo correntemente di 'società dell'informazione', ma la visione che l'informazione sia l'essenza della relazione e del commercio era ben presente a Marco Polo come a Cristoforo Colombo, e Dénis Diderot scrive nell'Encyclopédie: «Per commercio s'intende, nel senso generale, una comunicazione reciproca. Si applica più particolarmente alla comunicazione che gli uomini si fanno tra di loro dei prodotti delle loro terre e della loro industria».

La comunicazione è l'azienda: senza comunicazione l'azienda non esiste perché non ne esistono i presupposti per agire, come senza comunicazione non esistono possibilità di relazione sociale.

Si stabilisce così un fortissimo legame tra sicurezza e comunicazione d'impresa: senza sicurezza l'informazione dell'azienda non è affidabile, come senza fiducia non esiste commercio. Possiamo affermare che la sicurezza non garantisce semplicemente lo scambio dell'informazione, ma ne garantisce l'esistenza: senza sicurezza ci sono forse chiacchiere, ma non c'è certamente comunicazione d'impresa.

Porre con forza la questione del valore non deve indurre a una miope visione puramente economica: il riferimento al valore va inteso in senso ampio che vada a comprendere anche valori etici e ideologici.

Se non avessimo questo concetto di valore dovremmo dire, come in passato si diceva, che vanno protette solo le informazioni che trattano denaro, mentre è doveroso garantire la confidenzialità dell'informazione anche quando avviene tra due amici che

parlano del loro ristorante preferito, perché 'l'intimità' è un valore cui ciascun individuo ha pieno diritto.

1.1. La non-misurabilità della sicurezza dell'intangibile

Nel momento in cui riconosciamo il valore dell'intangibile, dobbiamo evitare la contraddizione di volerlo misurare con esattezza o di volerlo ricondurre a elementi decisionali che sono propri del mondo dei valori materiali. È logico non spendere per l'antifurto di un'automobile una cifra che risulti superiore al valore dell'automobile stessa, ma come decidere quando il valore non è quantificabile? In molte occasioni ci si sforza di convincere un riluttante cliente ad acquistare un nuovo sistema di sicurezza mostrandogli il calcolo del ROI o il costo rispetto al danno che potrebbe subire, come se il denaro giustificasse tutto: quanto vale l'infanzia violata di un sito pornografico? quanto vale la perdita di fiducia di un cliente, il suo fatturato? quello che non farà? quello che non farà fare agli amici a cui parlerà male di noi? quanto vale la vita che l'imprenditore ha speso per costruire la sua azienda? una cifra o un'altra farà la differenza?

La riduzione dell'equazione della sicurezza a puri valori monetari può diventare un grave limite che nasce da una visione ottusa, che non ci aiuta a capire e non ci fornisce strumenti interpretativi per un futuro che ci si para di fronte a lunghe falcate.

Anche se può prestare il fianco a molte critiche, il solo atteggiamento possibile parte da un qualcosa di indefinito che potremmo chiamare 'buon senso', che sembra fare a pugni con la logica binaria, ma che invece fa uscire il nostro ragionamento dalle secche dell'economicismo più becero.

Con lo sviluppo e la diffusione dei sistemi informativi che, grazie alla rete, sono usciti dai santuari delle sale macchine, il tema della sicurezza informatica, da materia esoterica per addetti ai lavori è diventata argomento di interesse comune e fonte di giusta preoccupazione dei singoli individui oltre che, com'è naturale, di aziende ed enti pubblici.

Con milioni di computer collegati e con sistemi mobili e sempre più veloci, c'è da domandarsi se il sistema nel suo complesso sia difendibile o se dovremo essere 'condannati' a un perenne stato di violazione e prevaricazione.

1.2. Certezze in un mondo incerto

Il bisogno di sicurezza, secondo la teoria dei bisogni di Maslow, è un bisogno primario che viene subito dopo il soddisfacimento dei bisogni fisiologici, è la condizione necessaria al fine di stabilire relazioni con gli altri, perché in un ambiente 'insicuro' non siamo a nostro agio e le emozioni hanno il sopravvento sulla ragione. La nostra fisiologia è stata progettata per reagire alle sensazioni di pericolo: produciamo adrenalina, aumentano i battiti cardiaci e poco importa se la minaccia sia oggettiva o solo immaginaria, l'istinto di sopravvivenza ha sempre il sopravvento, governato dalle componenti più profonde nell'encefalo.

Viviamo in un mondo di incertezze che sono cresciute e mutate con le trasformazioni sociali e chiediamo all'informatica certezze che non abbiamo nella nostra vita quotidiana. I dati INAIL parlano ancora oggi di oltre 1 milione di incidenti sul lavoro ogni anno, mentre gli incidenti domestici sono, ogni anno, più di 4 milioni e causano la morte, sempre ogni anno, di oltre 8.000 persone. Secondo l'Organizzazione Mondiale per la Sanità, ogni anno in Europa muoiono oltre 127.000 persone per incidenti stradali e 2,4 milioni restano ferite o rese disabili per lo stesso motivo. Sono cifre spaventose, riconducibili a una 'tecnologia', quella dell'automobile, che ha più di 100 anni e in cui le singole entità, cioè le automobili, hanno fatto sensazionali progressi in materia di sicurezza, ma in cui la complessità del sistema (strade, numero di auto in circolazione, numero degli utilizzatori, velocità media) produce effetti devastanti e non solo genera 'insicurezza', ma una vera e propria strage ogni anno.

La tecnologia dell'informazione sta seguendo percorsi simili, ma con una velocità esponenziale. I computer sono sempre più affidabili e sicuri, tuttavia l'ecosistema in cui interagiscono crea una condizione di pericolo costante. Il mondo dell'informatica, presentato come il mondo binario degli 1 e degli 0 in cui non esistono sfumature, ingenera inoltre una forte aspettativa di certezza e di prevedibilità e la convinzione del totale dominio dell'uomo sulla macchina. Ricordo che il padre della cibernetica italiana, il prof. Ceccato, parlando del computer lo chiamava «l'idiota fulmineo» perché, se istruito dall'uomo a fare una cosa sbagliata, la faceva comunque e sempre a velocità straordinaria. Chi oggi si occupa di sicurezza sa che la caratteristica dei sistemi interconnessi

è quella della imprevedibilità e che singole componenti pur affidabili, inserite in contesti sistemici, creano vulnerabilità estese.

1.3. L'incertezza dell'intangibile

A complicare la situazione si aggiungono alcuni caratteri propri della sicurezza informatica con cui dobbiamo fare i conti: ad esempio il principio secondo cui la sicurezza non esiste.

Non potremo, infatti, mai essere 'sicuri' al 100%, così come non possiamo aspettarci di vivere in eterno o di essere sempre in buona salute e, se è vero che non esiste in assoluto, possiamo dire che la sicurezza è la ricerca di un equilibrio dinamico, cioè sempre in movimento, tra apertura e chiusura, tra improvvisazione e regole, tra costi e danni.

La sicurezza inoltre non è una condizione oggettiva uguale per tutti, ma fa entrare in gioco importantissimi fattori emotivi e di vissuto personale che, a parità di situazione, portano ad azioni molto diverse fra loro. Si dice quindi che la sicurezza è un'emozione e le emozioni sono i motori dei comportamenti e dato che la sicurezza richiede specifici comportamenti e non solo tecnologie, richiede una forte coerenza nell'interazione fra i due: che senso ha una porta blindata se lascio la chiave nella toppa? Che senso ha una password lasciata in chiaro sul tavolo? Che senso ha avere in casa medicinali scaduti? Che senso ha un sistema antivirus se non viene aggiornato?

L'esigenza di comportamenti virtuosi e coerenti è poi il fattore determinante per la creazione di un ambiente complessivamente sicuro. Lo sa bene chi ha figli, che l'educazione passa principalmente attraverso gli esempi più che attraverso regole e prediche (che bisogna comunque fare), sulla cui utilità è lecito spesso dubitare. Così in ambito professionale non possiamo aspettarci il rispetto delle regole se siamo i primi a infrangerle e tanto più se la nostra posizione nella gerarchia aziendale è elevata.

Lo spostamento dei valori verso l'intangibile, sommato alla forte componente emozionale della sicurezza in generale, agisce da moltiplicatore anche per la sensazione di insicurezza che caratterizza soprattutto coloro che si affacciano alla rete e ai suoi servizi per la prima volta.

Le domande 'rivelatrici' di questo stato d'animo sono tipicamente: «ma posso dare i codici della mia carta di credito per fare

acquisti?», dimenticando che non è meno pericoloso del dare materialmente la nostra carta di credito a un cameriere che dopo qualche minuto torna con il conto e la ricevuta da firmare, oppure: «ma le telefonate in Internet sono sicure?», come se gli scandali recenti delle intercettazioni non ci avessero sufficientemente mostrato la violabilità di sistemi di comunicazione che usiamo da anni.

1.4. Il valore dell'identità

Nel mondo della rete siamo ormai abituati a rispondere alla domanda «Digita la tua login e la tua password». Spesso non si dà il giusto peso a questa azione che invece è densa di significati etici e filosofici, oltre che tecnologici. La domanda, infatti, può essere sintetizzata in: «Tu, chi sei?» e potremmo affermare sarcasticamente che l'uomo su questa domanda si interroga da oltre duemila anni senza trovare risposte convincenti.

Se è difficile dire con precisione 'chi siamo' nel mondo reale, forse ancora più difficile è poterlo definire nel mondo della comunicazione, ma la nostra identità nel mondo virtuale assume fattori che ne moltiplicano le forme e quindi la complessità e nel contempo ne amplificano il valore e la conseguente vulnerabilità.

Se inizialmente i codici di accesso servivano a identificare un operatore tecnologico seduto al terminale, oggi ci identificano individualmente e, in base a sistemi di profilazione e accordi di interconnessione, le nostre richieste vengono interpretate, esaudite e memorizzate, ma spesso anche ipotizzate e anticipate.

La molteplicità dei sistemi e l'impossibilità pratica di realizzare il sogno del 'Single Sign-on', i sistemi di identificazione univoca per tutti i sistemi, ci portano ad attivare identità molteplici, e sempre più spesso siamo confusi da login e password che abbiamo scelto o ricevuto senza pensarci troppo, non capendo che dietro a quei codici si cela un valore elevatissimo.

Tralasciando le implicazioni psicologiche e filosofiche, nel mondo reale ci rendiamo conto del valore dell'identità, solo quando siamo obbligati a provarla oggettivamente, ad esempio da un notaio per una compravendita, o, peggio, se accusati ingiustamente di un reato. Sappiamo bene che spesso il danno più grave, se perdiamo o ci viene rubato il portafoglio, non è nei pochi euro che conteneva, ma nel dover rifare i documenti, bloccare i banco-

mat e le carte di credito, chiedere una nuova tessera sanitaria o della biblioteca comunale.

Nel mondo virtuale il primo problema è di capire se 'ci hanno rubato il portafoglio', se cioè la nostra identità è stata compromessa e come impedirne gli abusi; se invece 'perdiamo il portafoglio' perché si guasta il disco che conteneva tutte le nostre login e password, ricostruire le nostre identità digitali diventa un processo lungo e noioso.

Difendere la nostra identità digitale è quindi una priorità assoluta anche perché, se possiamo dire che non c'è valore più alto della tutela della nostra intimità, della nostra dignità, della nostra sfera familiare, la necessità del mercato di concludere il più velocemente possibile una transazione economica tende a banalizzare il trattamento delle informazioni che ci riguardano.

Si evidenzia una forte contraddizione: da un lato si esalta l'individuo, il servizio mirato per il singolo, la vittoria del soggetto sulla massa, ma si scopre immediatamente che non c'è alcun rispetto per l'individuo-persona, per ciò che siamo veramente. È il medesimo inganno che hanno lanciato i primi sistemi di direct marketing che ci facevano arrivare a casa lettere fintamente personalizzate: «Questo messaggio è solo per lei, cara signora GIGI TAGLIAPIETRA», talvolta con ridicoli errori o con proposte impossibili, come quando hanno proposto a mio figlio di sette anni un viaggio ai Caraibi.

Siamo in una nuova era, non c'è dubbio, il web che ora è chiamato web 2.0, a significare il salto di qualità, offre sempre più servizi personalizzati e realizzati direttamente dalla relazione dei partecipanti, servizi che nascono dal ruolo di utenti che diventano a loro volta fornitori di informazioni, come nel caso di YouTube, di Flickr, dei blog e dei tanti servizi che vivono di reti sociali.

1.5. Le minacce specifiche

Nella vita reale, carpire la nostra identità 'formale' e cioè i nostri documenti non è complesso, mentre è più difficile, anche se non impossibile, impersonarci fisicamente. In rete, una volta catturate le nostre credenziali, chi ne dispone può, di fatto, agire in nostro nome e per nostro conto e non stupisce che uno dei fenomeni criminali più diffusi sia il 'furto di identità' che, secondo le stime presentate alla RSA Conference dal Presidente di Verisign, è costa-

to lo scorso anno negli Stati Uniti più di 15 miliardi di dollari e ha colpito oltre 10 milioni di soggetti.

Il primo periodo di questa nuova era ha visto la diffusione di fenomeni come il phishing (la cattura di credenziali e password con messaggi fintamente provenienti da banche o istituzioni riconoscibili), che potremmo paragonare al finto impiegato dell'Inps che, con la scusa di controllare la pensione del malcapitato, gli ruba invece gli ori di famiglia.

I primi a essere colpiti sono stati i sistemi bancari che hanno scoperto, di conseguenza, la perniciosità di queste forme di truffa. In effetti, non si tratta di attacchi portati ai sistemi della banca, solitamente ben protetti, ma a quelli molto meno difesi dei loro clienti.

Si tratta inoltre di attacchi che, carpendo la buona fede della vittima, non sono difendibili con tecnologie, almeno non in senso stretto, ma che richiedono un'educazione al comportamento corretto e all'attenzione in forma assolutamente capillare.

La risposta al phishing è costata proporzionalmente molto cara alle banche perché, se è vero come sottolineano i dati ABI che le entità in gioco non sono numericamente rilevanti, è vero che le contromisure messe in atto (sms ai clienti per ogni bonifico effettuato, sistemi di data-mining che controllano movimentazioni anomale, interconnessioni con l'Interpol) hanno avuto costi organizzativi altissimi.

Il phishing ha evidenziato nella sfera privata la consapevolezza che la protezione dell''altro', in questo caso del cliente, è interesse primario di chi si occupa di sicurezza.

I nuovi attacchi non solo si caratterizzano per la sofisticazione o per la 'cattiveria', ma per un deciso abbassamento della dimensione aziendale del sistema attaccato. Se in passato le vittime predestinate erano i grandi sistemi governativi e quelli di banche e grandi aziende, assistiamo oggi a due fenomeni paralleli.

Il primo è che molti degli attacchi lavorano sulla logica dei grandi numeri e quindi sono del tutto inconsapevoli della reale identità della potenziale vittima e in questo caso i più esposti sono proprio i sistemi delle piccole e medie aziende e quelli dei singoli individui. È il caso dello spam o di tutte le forme di distribuzione di massa di codici maligni.

Ma sempre più spesso sono denunciate forme di phishing mirato a catturare le informazioni che vengono date a entità molto

piccole, il negozio sotto casa, piuttosto che l'associazione non profit di cui si è membri, nell'assunto che le persone tendano a utilizzare le medesime login e le medesime password anche nei sistemi più grandi.

1.6. Nuove minacce e nuovi bersagli

Un ulteriore elemento di cambiamento riguarda il mondo dell'hacking che è stato in gran parte sostituito dall'attacco eseguito da veri e propri criminali. Pekka Himanen (2001), consulente del governo finlandese per i temi informatici, sottolineava come fosse importante comprendere che le motivazioni che spingono gli hacker alla compromissione di un sistema non fossero necessariamente quelle che animano invece chi governa tali sistemi e che provare a comprendere il fenomeno con la metrica, ad esempio, del denaro, porta davvero lontano dalla realtà.

Va ricordato, per inciso, che il termine hacker, che in italiano si potrebbe tradurre con 'smanettone', non è sinonimo di criminale, anche se oggi il termine ha assunto nell'immaginario collettivo una connotazione negativa, tanto che, per operare un nuovo distinguo, si parla di ethical hacker per identificare quelli che rispondono comunque a un mondo di 'valori' e per distinguerli da chi ne è privo.

Negli ultimi due anni, la situazione è drasticamente cambiata, come hanno evidenziato tutti gli interventi più autorevoli alla RSA Conference, la conferenza annuale sulla sicurezza informatica che si tiene ogni anno a San Francisco. Siamo passati da un periodo 'epico' in cui l'hacker voleva compiere gesti eclatanti per avere notorietà, a un periodo più becero, quello attuale, in cui l'attacco ha finalità meramente criminali ed economiche e l'attaccante desidera fortemente conservare l'anonimato.

Ma quello che è drasticamente cambiato è il modello 'malattia-medicina' cui facevano riferimento molti degli interventi di adeguamento del software alle possibili vulnerabilità. In questo modello concettuale, una volta identificata un'anomalia o una disfunzione, veniva prodotto un aggiornamento che l'utente doveva installare: come se, riscontrata una malattia, venisse identificato il vaccino appropriato.

Il modello funzionava fino a che il tempo tra la scoperta del fattore di rischio, la predisposizione della contromisura e la distri-

buzione e installazione degli aggiornamenti era sufficientemente lungo.

Già dalla diffusione del 'Code Red' nel 2001, l'istituto CAIDA (*www.caida.org*) aveva evidenziato che la compromissione di oltre 300 mila sistemi era avvenuta in 14 ore, mentre il worm Slammer del 2003 in meno di 10 minuti ha colpito il 90% dei potenziali bersagli e in entrambi i casi erano pur sempre disponibili 'vaccini' in quanto le vulnerabilità erano note da tempo.

La pericolosità non è quindi nel 'virus', quanto nella sua dinamica di propagazione e la situazione si è ulteriormente evoluta. Oggi si parla di Zero-day attack, cioè di attacchi che sfruttano vulnerabilità ancora non note e di cui pertanto non esiste vaccino e la velocità di propagazione di un codice maligno è tale per cui il fattore tempo diventa insormontabile.

Ma un fattore di ulteriore criticità riguarda la presenza di sistemi informativi come parte integrante di sistemi di produzione certificati; pensiamo ad esempio all'industria chimica o farmaceutica, in cui un cambiamento di componenti del sistema deve sottostare a precise norme e procedure di validazione che in taluni casi richiedono mesi: com'è possibile in questi ambienti aggiornare i sistemi per i quali sono realizzati aggiornamenti ogni 2-3 settimane?

Viviane Reding, Commissario europeo alla Società dell'Informazione, nel suo intervento di apertura alla conferenza europea sulla sicurezza che si è tenuta a Roma nel 2006, ha ritenuto doveroso richiamare le aziende produttrici di software a una maggiore qualità nei prodotti che rilasciano abbandonando la forsennata corsa al 'rilascio' ad ogni costo.

Ma come è stato per la SARS o le altre possibili pandemie, dobbiamo adottare nuove strategie che, pur seguendo la ricerca di vaccini e contromisure, si avvalgano di regole comportamentali diffuse di igiene e controllo a livello capillare perché la sfida non è quella di affrontare i virus e le minacce note, ma creare un sistema che sappia rispondere tempestivamente a forme di attacco del tutto ignote e imprevedibili.

2. *La posta in gioco*

Il processo di smaterializzazione dei valori non è un processo omogeneo e coerente, nel senso che non tutti i valori intangibili

aumentano, anzi taluni addirittura sono banalizzati. Il caso più rilevante è quello della posta elettronica, assieme al web, la vera 'killer application' di quest'ultimo decennio, in cui un valore storicamente elevato (la scrittura e la confidenza interpersonale) si dissolve seguendo una sorta di legge dell'abbondanza, in cui il valore cala al crescere della disponibilità, mentre al contrario, proprio per la sua pervasività, la posta elettronica assume valori strategici ed etici sempre più elevati.

2.1. Un mondo di lettere

L'utilizzo della scrittura segna uno dei grandi passi della civiltà umana e la successiva invenzione della stampa a caratteri mobili apre alla conoscenza un orizzonte i cui effetti sono quelli che oggi conosciamo. La scrittura non è solo la possibilità di tramandare fedelmente storie, leggi e poesie, è stata anche potere e valore: potere perché gli imperatori usano la scrittura per far conoscere i propri voleri ai sudditi di regni sconfinati e valore perché usano la scrittura per tramandare ai posteri la propria vita di semidei.

Ma la scrittura non è solo scettro dei potenti, la statua dello Scriba seduto esposta al Louvre è simbolo di un mondo: la figura non è fisicamente imponente, ma il 'potere dell'intangibile' è tutto nei suoi occhi, quel piccolo uomo è il tramite per un mondo inaccessibile ai più. La scrittura assumeva il valore di eternizzare le idee e i voleri: «Verba volant, scripta manent» ci ricorda come il contrasto tra lo svolazzo delle parole e la permanenza dello scritto era ben presente nell'immaginario collettivo. Lo scritto era impegno, contratto, proiezione di se stessi. Non solo il racconto delle gesta dei potenti, ma fin da subito la poesia, il racconto di sé e il racconto epistolare danno alla scrittura un valore simbolico e reale da tutti percepito e rispettato. Nell'arco di pochi anni siamo passati da un grande valore a un dissolvimento di tale valore: ma è una percezione o una reale perdita di valore?

2.2. La posta oggi

Quando si pensa alla posta elettronica si pensa spesso a un servizio di assoluta marginalità rispetto alle applicazioni strategiche d'azienda, un servizio generalmente gratuito, offerto in 'omaggio' purché si acquistino altre cose. Siamo lontani dalla eroica figura del pony express, eppure la posta elettronica rappresenta

oggi per le aziende un sistema di comunicazione assolutamente indispensabile alla vita stessa dell'impresa.

I sistemi di e-mail hanno sconvolto i processi formali e velocizzato i contatti tra soggetti e imprese e tra gli individui e i loro agglomerati sociali. La scrittura, che aveva dominato la comunicazione per oltre duemila anni e che era stata soppiantata dalla comunicazione verbale resa possibile dalla telefonia (e più recentemente dalla telefonia mobile), torna in auge con la posta elettronica, con gli sms e le chat.

Ma il ritorno della scrittura non ha portato con sé un recupero della consapevolezza del valore proprio della scrittura, anzi pare averlo del tutto banalizzato: basta però un blocco della rete, un guasto a un mail server per renderci conto di quanto preziosa sia questa risorsa.

2.3. La metafora dell'acqua

Anche con l'acqua abbiamo atteggiamenti contraddittori: siamo un paese con grandi risorse idriche eppure siamo il secondo consumatore mondiale di acqua in bottiglia, con ben 5 miliardi di bottiglie l'anno, oltre 170 litri pro capite (fonte: Annuario 2002/2003 delle acque minerali e di sorgente Italia).

Perché paghiamo 500 volte di più qualcosa che ci piove addirittura addosso? Perché sappiamo che è un elemento indispensabile alla nostra vita e l'acqua, per essere utile al nostro organismo, deve essere filtrata da agenti patogeni e deve essere disponibile in qualsiasi momento: a casa, in viaggio, mentre facciamo sport o stiamo sdraiati al sole.

Come l'acqua anche la posta, perché sia utile alla vita dell'impresa, deve essere filtrata da contenuti dannosi, disponibile nei momenti critici, accessibile quando si è lontani. I mail server sono oggi esposti ad attacchi continui e sono veicolo involontario di diffusione di virus e worm anche perché ci si è dimenticati di quanto sia importante, da sempre, il 'presidio delle fonti': avere controllo diretto o da parte di nostri sicuri alleati delle nostre risorse primarie.

Lo scopo della sicurezza informatica è quello di garantire che i sistemi chiave dell'azienda siano protetti per consentire all'azienda stessa di sviluppare la propria missione: quale sistema è più cruciale e più 'indifeso' se non proprio la posta?

L'acqua ci sembra una risorsa infinita, ma già si prefigura un futuro in cui potrebbe diventare una risorsa più preziosa di quanto non sia oggi il petrolio; ci piove addosso eppure non ci basta mai.

Siamo fatti per gran parte di acqua come per gran parte siamo fatti di relazioni e comunicazioni e non dobbiamo dimenticarlo: quel messaggio di posta elettronica è un pezzo di noi, un pezzo della nostra identità digitale, una goccia del nostro sudore.

2.4. Privatezza e autenticità

Gli attentati di Londra dello scorso anno hanno richiamato l'attenzione sulla rilevanza della posta elettronica anche come 'arma' utilizzata dai gruppi terroristici e criminali per coordinare le loro iniziative. Come sempre accade sull'onda di eventi drammatici, sono state fatte proposte per limitare e controllare l'utilizzo indiscriminato di strumenti che proprio per la loro natura di libertà rappresentano una minaccia in un utilizzo malevolo.

Torna sui tavoli dei legislatori il tema della definizione degli ambiti in cui 'violare' il segreto della corrispondenza – non solo elettronica –, e il grande rischio è di prendere provvedimenti 'spettacolo' ma del tutto inefficaci sul piano pratico.

Qualcuno ha in mente un nuovo Echelon per la posta? Uno strumento per analizzare 'on the fly' tutti i miliardi di messaggi che circolano in rete? Troppo complesso? Allora si chiede di archiviare tutti i messaggi per poterli analizzare successivamente! Avete idea di cosa stiamo parlando in termini dimensionali? Cosa potremmo dimostrare in termini legali: che un determinato giorno il signor Rossi ha scritto al signor Bianchi? Ma era davvero il signor Rossi? O qualcuno da un certo indirizzo IP con una certa login? O qualcuno che ha manomesso tali informazioni?

L'autenticazione degli interlocutori è un elemento fondamentale da tenere in considerazione e, se l'anonimato è stato un cavallo di battaglia a difesa delle libertà individuali, oggi l'identificazione certa di mittenti e destinatari rappresenta un passaggio cruciale per contenere fenomeni come lo spam o il Phishing.

Non dobbiamo dimenticare che dietro a questi ragionamenti esistono punti di vista molto diversi e 'storie sociali' del tutto diversi: si pensi al fatto che l'anagrafe comunale o la carta d'identità, che per

noi sono strumenti di convivenza civile, in alcuni settori del mondo anglosassone sono visti come minaccia alla libertà personale.

Tra i due estremi, tra Echelon e «puoi anche essere un cane e nessuno lo saprà», di certo occorre trovare soluzioni concrete e ragionevoli che siano effettivamente utili al contrasto della criminalità e siano nel contempo utili a ciascuno di noi per utilizzare la posta in modo tutelato.

La tutela della corrispondenza è scritta nelle carte costituzionali a ricordarci il valore supremo della dignità personale che è insita in un messaggio di chi ci scrive e dell'intimità inviolabile che rappresentiamo in quanto destinatari.

2.5. Rispetto e valori non solo tecnologie

L'uso, spesso smodato, delle e-mail ci ha fatto perdere di vista un altro importantissimo aspetto: quello della autorevolezza del 'mezzo' e la conservazione dei documenti nel tempo.

La scrittura di una lettera, rispetto alla comunicazione verbale, serviva non solo a rendere formale e attenta la comunicazione ma a consentire, nel tempo, la ricostruzione di un dialogo e delle sue ragioni, economiche o sentimentali che fossero. La 'carta intestata' era un sinonimo di autenticità e la sua scomparsa nel mondo delle e-mail pone temi analoghi a quelli legati all'autenticazione degli individui.

Se in passato esisteva la 'sacralità del timbro' e la consapevolezza che scrivere qualcosa sulla carta intestata aziendale implicasse assunzione di responsabilità importanti, la struttura 'da-a-cc-argomento-testo' ci allontana dall'idea che stiamo compiendo un atto formalmente rilevante e se è vero che «Il mezzo è il messaggio», come diceva McLuhan, il senso di ciò che diciamo è più nel mezzo che nel contenuto.

Oggi la posta elettronica crea una comunicazione diretta e velocissima ma rende assolutamente problematica per un'organizzazione la ricostruzione di processi e di impegni con rilevanti conseguenze economiche e giuridiche.

Come garantire la conservazione nel tempo dei messaggi, come garantire la facile ricostruzione delle sequenze di dialogo, come ritrovare ordini e conferme in questo mondo sempre più effimero? Come mantenere l'unitarietà quando la posta, anche d'impresa, è distribuita nelle caselle personali degli utenti e sparpa-

gliata su centinaia di hard disk? Si possono trovare soluzioni tecnologiche, ma potrebbero non essere sufficienti: la risposta deve essere anche vista in termini di rivalutazione del valore che ciascuno di noi dà alla comunicazione scritta. Se non diamo valore alle cose, difficilmente troveremo in noi le ragioni per difenderle o per proteggerle e nemmeno comprenderemo gli sforzi che altri vorranno fare per il nostro bene.

Dobbiamo aiutare gli utenti a comprendere che le nostre caselle di posta non sono solo 'nostre', se siamo in azienda, anche se lo siamo solo virtualmente; dobbiamo vedere i messaggi che abbiamo nelle nostre caselle come la posta cartacea che una volta avevamo fisicamente sul tavolo: prima di gettarla nel cestino o di confonderla con altri documenti ci abbiamo sempre riflettuto.

Anche i messaggi non sono solo 'nostri': un messaggio che riceviamo è innanzitutto di chi ce lo ha mandato e non è corretto inoltrarlo ad altri senza il consenso dell'autore. Lo fareste con una lettera scritta a mano, magari in cui qualcuno che si fida di voi vi apre il suo cuore? La posta è preziosa perché tratta materiale prezioso: le nostre parole sono un pezzo di noi, noi nella nostra relazione con gli altri.

La posta elettronica è importante per noi come individui e nel contempo una risorsa aziendale strategica e vitale, il diritto alla confidenzialità e il rispetto sono regole sociali che non scompaiono con Internet o con il wi-fi.

La posta elettronica è davvero come l'acqua: non continuerà a uscire dai rubinetti se ciascuno di noi non la tratterà come un bene prezioso. Le inondazioni e gli tsunami sono lì ogni tanto a ricordarci anche la sua potenza devastante.

3. *Unità e sistemi complessi*

C'è da domandarsi sinceramente se sia difendibile un sistema che ha visto, nel 2005, 155 milioni di nuovi utenti e che avrà nei prossimi 4 anni, secondo alcune stime, 2 miliardi di utenti mobili e 2 miliardi di utenze broadband. C'è da preoccuparsi vedendo che il mercato della sicurezza (dati statunitensi) è stimato in 18 miliardi di dollari con un tasso di crescita del 15-18% l'anno, mentre l'ammontare dei danni per incidenti di sicurezza è stimato in 50 mi-

liardi di dollari con un tasso di crescita del 45% annuo (fonte: RSA Conference Keynote).

Lasciando all'eterno confronto tra ottimisti e pessimisti la lettura del futuro, credo si debba affermare con forza che la rete e l'informazione che in essa circola sono risorse preziose per tutti noi e che vanno difese con determinazione, anche se sarà un impegno non semplice e non di breve durata.

Molte delle iniziative dovranno partire da un vecchio slogan della rete: «think globally, act locally», comprendendo che la nostra azione può portare benefici o pericoli all'intero sistema, ma che ciascuno deve agire partendo dal proprio ambito diretto.

3.1. Sicurezza come ecosistema

Per comprendere la complessità del tema della sicurezza informatica dobbiamo riferirci per analogia ad altri sistemi complessi e, per paradossale che possa sembrare, dobbiamo pensare all'insieme dei sistemi informativi non come a una grande 'macchina' ma come a un organismo 'vivente'.

Le reti informatiche assumono infatti caratteristiche molto simili a quelle degli altri ecosistemi e in questo senso sono molto interessanti le osservazioni di Mark Buchanan nel suo libro *Nexus* (2004) che ha un sottotitolo molto intrigante: 'Perché la natura, la società, l'economia, la comunicazione funzionano allo stesso modo'.

Estremamente interessante nella riflessione di Buchanan l'identificazione dei punti di forza e di debolezza dei sistemi interconnessi e di come esistano delle soglie di autorigenerazione, ma anche soglie oltre le quali il sistema collassa e propaga la distruzione.

La struttura a rete non è per la verità una conseguenza solo del fenomeno internet, ma una caratteristica propria di come i calcolatori siano stati progettati e costruiti, con la concezione di 'sistema'.

Internet 'esplode' all'esterno e amplifica in termini dimensionali le componenti già presenti nella singola macchina. Per comprendere questo concetto si immagini per un attimo cosa vedrebbe un microbo che si muovesse in un computer: vedrebbe tante unità elaborative connesse fra loro attraverso un 'filo' (le connessioni della piastra madre) e un continuo scambio di dati tra diver-

se unità che memorizzano ed elaborano informazioni. Come in un frattale ogni singolo elemento è lo specchio del tutto – e la complessità, con la relativa bellezza, sta nella moltiplicazione esponenziale – così nel singolo sistema computer sono presenti le caratteristiche dell'intero sistema della rete: guardare una felce o un cavolfiore che sono simboli naturali di questo concetto può aiutare a comprendere come il singolo e il tutto siano strettamente correlati.

La conseguenza di questo punto di vista è che la rete è un ecosistema di cui non solo fanno parte le macchine, ma anche gli utenti che con esse interagiscono e, quando ci poniamo il dilemma di come difenderlo, di come 'garantirne la vita', dobbiamo essere capaci di sviluppare approcci sistemici, perché qualunque tentativo meccanicistico e lineare porterebbe a soluzioni temporanee e a problemi di medio e lungo periodo come già abbiamo potuto sperimentare nell'affrontare i temi ambientali.

Un altro campo da cui possiamo attingere concetti innovativi è quello della fisica delle particelle; esso ci ha aperto un mondo affascinante, nel quale le contraddizioni sono parte di ciò che osserviamo: «Se la fisica non vi stupisce», diceva Niels Bohr, «vuol dire che non l'avete capita». La fisica del secolo scorso, rispetto a quella di Newton, ha detto che l'osservatore non è un'entità estranea al fenomeno, ma che è parte integrante dell'esperimento e del fenomeno osservato. È un punto di fondamentale importanza nell'approccio alla sicurezza, perché ci mette nella condizione di capire che siamo noi stessi parte del problema, con i nostri pregiudizi, con le nostre emozioni, con la nostra interazione con il mondo delle macchine.

3.2. Affrontare la complessità

Lo studio dei modi per affrontare 'problemi complessi' è di per sé una disciplina affascinante che ci porta ad assumere approcci del tutto innovativi e a volte controintuitivi rispetto a ciò che siamo soliti dire o fare. Horst Rittel e Melvin Webber nel 1973 presentarono la teoria dei cosiddetti 'wicked problems', i problemi ingarbugliati (vedi http://www.swemorph.com/wp.html), in cui propongono un approccio metodologico per quei problemi di cui non è possibile nemmeno definire i contorni se non si inizia ad affrontarli. Sono i problemi che devono esaminare gli urbani-

sti o gli studiosi di scienze sociali e sono oggi i problemi di chi si occupa di sicurezza della rete.

La metodologia, poi ulteriormente sviluppata da Jeff Conklin (http://cognexus.org/), può essere applicata in generale nell'affrontare problemi organizzativi complessi, ma è indispensabile nella macrodefinizione delle soluzioni di sicurezza perché ottiene come risultato una mappatura delle motivazioni che ci portano a prendere specifiche decisioni.

In caso di incidente ci dobbiamo domandare: perché avevamo fatto quella determinata scelta? E quando cambiamo una delle decisioni dobbiamo sempre avere ben chiara la mappa dell'intero sistema per non aprire nuove falle.

Sono infatti disastrose le azioni che portano a quelle che potremmo definire 'tentate soluzioni' o meglio soluzioni che nel risolvere un problema localizzato ne creano uno ben più devastante.

Non solo siamo 'condannati' a un approccio sistemico nell'affrontare oggi i temi della sicurezza delle informazioni, ma lo saremo sempre di più vista l'evoluzione che la rete sta seguendo.

3.3. Teoria della paura

Se fare leva sui valori è sempre l'approccio migliore, bisogna invece utilizzare grande cautela con la leva della paura. Tutta la comunicazione relativa alla sicurezza, salvo poche eccezioni, si basa sulla paura: paura di perdere qualcosa, paura dell'estraneo, paura dell'ignoto.

È una leva emozionale forte ma che introduce un pericoloso effetto collaterale: una persona spaventata non agisce razionalmente e spesso compie gesti inconsulti. Se il nostro scopo è quello di ottenere comportamenti coerenti e virtuosi, di attuare abitudini consapevoli e attente, stiamo andando nella direzione sbagliata.

Presentare il mondo della sicurezza solo come un mondo di buoni e cattivi, di criminali e pulzelle indifese è anche fuorviante. Ci sono rischi gravissimi che derivano da incuria o da fragilità intrinseca che non sono meno minacciosi di un attacco di cyberterroristi. Risvegliare la paura è pericoloso, far comprendere il rischio è altra cosa: la prima è un'apparente facile scorciatoia, la seconda richiede tempo e condivisione di valori.

Nella comunicazione pubblicitaria, ad esempio, la paura è utilizzata solo per destare l'attenzione iniziale di utenti totalmente inconsapevoli, come se lanciassimo un grido di attenzione a un bambino che sta attraversando la strada senza guardare. Tutta la comunicazione successiva è invece rassicurante, coinvolgente, addirittura scherzosa per sdrammatizzare ma sempre con un percorso che va dall'emozione alla ragione.

Sicurezza è emozione, dice il secondo principio; ma esagerare con l'emozione porta all'infarto.

3.4. Come si insegna la sicurezza

Se una corretta comunicazione è un fattore vincente, altrettanto lo è un approccio aperto e innovativo alla formazione. Non si tratta di formare degli specialisti, si tratta di creare una consapevolezza diffusa della posta in gioco e del ruolo che ciascuno è chiamato a compiere con comportamenti corretti sia nell'attività professionale sia nella sfera privata.

Perché un progetto di formazione diffusa abbia successo, bisogna innanzitutto che sia guidato e condiviso al più alto livello di direzione, coinvolgendo tutti i reparti e puntando all'informazione di tutti i collaboratori e non solo a quelli direttamente impegnati nell'uso di computer.

Un fattore critico, forse il più critico, è quello della continuità, perché è facile lanciare una campagna, attivare un corso on-line, stampare una brochure o un cd, ma è difficile mantenere nel tempo l'iniziativa, non solo per assicurare la formazione dei neoassunti, ma anche e soprattutto per mantenere alta l'attenzione e non cadere nelle braccia del grande nemico della sicurezza che è l'abitudine.

La diffusione dei computer nelle famiglie ha notevolmente innalzato l'interesse dei singoli all'acquisizione di conoscenze specifiche in materia di sicurezza e questa condizione va utilizzata per aumentare l'efficacia dei processi formativi. Anziché una noiosa sequenza di slide che spieghi il regolamento interno all'uso dei sistemi in base ai dettami della legge sulla privacy, è cento volte più efficace partire dalle esigenze di protezione della propria intimità, di quella dei propri figli e far comprendere che un analogo comportamento rispettoso della confidenzialità va tenuto anche quando si trattano informazioni relative a clienti e fornitori.

Bisogna fare in modo che il processo di formazione trasformi i collaboratori in attivi protagonisti del sistema di difesa e non in semplici esecutori di norme, facendo loro comprendere come l'informazione sia un bene prezioso da cui dipende anche la continuità e la difesa del loro lavoro.

Bisogna infine utilizzare un insieme di mezzi in sinergia fra loro, ricordando che il computer (cd o corso on-line) è il meno costoso e logisticamente più immediato, ma che spesso rappresenta per l'utilizzatore una barriera psicologica ed emotiva che può vanificare lo sforzo di comunicazione. La soluzione è quella di utilizzare l'insieme di mezzi per fare in modo che ciascuno trovi poi quello più consono a sé e che sfrutti strutture esistenti e abitudini di fruizione consolidate.

Puntare sull'alfabetizzazione diffusa non vuol dire dimenticare la formazione tecnica specifica dei professionisti chiamati a gestire i sistemi di sicurezza aziendale; le attività anzi devono essere svolte in parallelo.

I professionisti della sicurezza aziendale devono trovare comprensione da parte degli utenti quando chiedono loro di rispettare le disposizioni tecniche che vengono impartite e devono ricevere tempestivamente feedback e segnalazioni da parte di un'utenza attenta e responsabile.

Nella formazione dei professionisti sono di grande aiuto le certificazioni specifiche che garantiscono il completamento di precisi percorsi formativi, anche se non dobbiamo dimenticare che molte di esse attestano la comprensione di un insieme di nozioni acquisite ma non ci garantiscono il comportamento in caso di emergenza.

Un limite dei sistemi internazionali di certificazione è che essi riproducono modelli culturali dei sistemi scolastici di cui sono parte. Ecco quindi l'esasperazione del test, dei punteggi, delle metriche all'americana, che vanno bene per la gestione di apparati, ma che mal si adattano a tutto ciò che è stato affermato a proposito delle nuove sfide della sicurezza. Queste richiedono invece estro, creatività, capacità di operare in condizioni di emergenza. Tutte qualità mediterranee difficilmente valutabili in un test a crocette.

3.5. Sicurezza ed etica

La tecnologia è del tutto inefficace in ambienti privi di un solido sistema di valori etici condivisi ed è altresì inefficace quando deve

affrontare situazioni impreviste o per le quali non è stata progettata. Se il rispetto della confidenzialità non è un valore etico condiviso dalle persone e dalla direzione aziendale, non c'è crittografia che tenga; se il rispetto costituzionale della segretezza della corrispondenza non è sentito come un imperativo, non esistono sistemi tecnologici che impediscano il trattamento della posta elettronica nel totale disprezzo delle più elementari norme di buona educazione.

Forti valori etici sono richiesti in particolare a chi gestisce al più alto livello i sistemi di sicurezza perché ne diviene il garante e il fiduciario nei confronti dei propri colleghi e nei confronti della direzione: avere le chiavi di accesso ai segreti più alti deve fare coppia con un grande senso di responsabilità. Al di là dei propri valori etici esiste un mondo di leggi che chi si occupa di sicurezza deve rispettare e far rispettare, dalla legge sulla privacy allo statuto dei lavoratori, dalla tutela del diritto d'autore alla legge sulla concorrenza. Possono esistere situazioni in cui le scelte vanno compiute in assenza di specifiche norme ed ecco quindi la necessità di riferirsi a valori etici generali o situazioni di conflitto tra la norma e le proprie convinzioni. Del tema si era già occupato Sofocle nella tragedia di Antigone e a 2500 anni di distanza la risposta, qualunque essa sia, non è detto sia quella giusta.

Un approccio principalmente etico riguarda la tutela delle persone più esposte ai rischi della rete: anziani, bambini, minoranze etniche e culturali. Già più di dieci anni fa, con la carta dei diritti dei minori in rete, redatta in collaborazione con il prof. Scaparro, dicevamo che bisognava innanzitutto creare attorno a loro un mondo di diritti, di cui i bambini erano primariamente portatori e in primo luogo il diritto di avere attorno a sé adulti responsabili.

Quello che è difficile ottenere in rete è l'assunzione di responsabilità, perché si ritiene che l'anonimato sia la sola forma che garantisca la privacy; ma c'è molto da discutere su questo punto di vista che nella cultura anglosassone considera la carta di identità una minaccia alla privacy. Al contrario, secondo quanto esposto, si ritiene che la privatezza della comunicazione debba essere garantita senza ricorrere all'anonimato e che, anzi, chi esprime pubblicamente le proprie opinioni debba assumerne la responsabilità; da questo punto di vista il modello di RCM e di Onde rimangono due realtà concrete che a distanza di dodici anni conferma-

no il legame tra tutela e identificazione dei partecipanti a una comunità.

3.6. Sicurezza e libertà

Lo scontro tra sicurezza e privatezza è stato particolarmente acceso nel dopo 11 settembre, quando si è teorizzato il concetto che per avere maggiore sicurezza occorreva rinunciare ad alcuni aspetti di privacy.

Come ha più volte sostenuto il prof. Danilo Bruschi, presidente onorario del Clusit, si tratta di una questione mal posta, che in realtà nasconde due finalità meno nobili: la prima che approfitta della situazione per ridurre la sfera delle libertà individuali e la seconda che intende sacrificare la privacy per motivi di costo di sviluppo di sistemi di controllo che siano anche rispettosi. Se riteniamo che la privacy sia un valore etico primario dobbiamo allora investire le risorse adeguate per sviluppare soluzioni appropriate.

Analogo percorso sta seguendo il dibattito molto acceso in questi mesi che vede la sicurezza tra gli argomenti utilizzati a sostegno di chi vorrebbe modificare alcuni degli aspetti che regolano il funzionamento di Internet. Il tema è quello della neutralità della rete, che qualcuno sostiene debba essere limitata per garantire maggiore sicurezza ai singoli e alle nazioni.

Invece, il ragionamento deve essere esattamente l'opposto: la sicurezza deve servire a garantire la fruibilità di uno spazio condiviso e garantire che non avvengano pratiche discriminatorie, così come la polizia ha il compito di assicurare che tutti possano fruire liberamente e rispettosamente del giardino pubblico.

È un compito arduo, come arduo è sempre il mantenimento della libertà che non voglia ricorrere alla scorciatoia della violenza o della dittatura; ma è un compito che chi si occupa di sicurezza deve sentire come un impegno primario, perché ciò che viene fatto nella rete aziendale si riverbera nella rete complessiva.

3.7. Cosa fare

Non è facile rispondere alla domanda finale che dice: ma in pratica, cosa dobbiamo fare?

Non è facile, perché non c'è una sola risposta e perché, come dice la teoria dei wicked problems, non ci sono soluzioni vero-falso, ma piuttosto migliore-peggiore, per cui possiamo dare alcune

indicazioni su cosa sarebbe meglio fare viste le condizioni attuali e le tendenze in atto. Di certo dobbiamo comprendere che la smaterializzazione del valore non ne ha diminuito l'entità, anzi, ha portato alla ribalta del valore entità inestimabili come la libertà, la dignità, il rispetto e dobbiamo altresì comprendere che 'la comunicazione siamo noi' e che proteggerla significa svilupparla e fare crescere e proteggere noi stessi.

È un compito impossibile da affrontare da soli, ma che richiede impegno individuale. Innanzitutto, la sicurezza va affrontata in termini collaborativi superando l'approccio egoistico della ricerca della propria esclusiva sicurezza: vale la pena ricordare che sarebbe inutile essere la sola azienda sicura in un mondo che avesse fatto 'morire' tutti i clienti e i fornitori.

La visione della collaborazione come strumento di crescita dell'economia e della sicurezza in particolare ha portato allo sviluppo di sistemi di scambio di informazioni anche tra concorrenti che hanno compreso come la difesa della rete sia una pre-condizione perché poi lo scontro avvenga sui contenuti delle diverse offerte.

È come se avessimo compreso che la difesa del terreno di gioco non è un fatto competitivo di cui si avvantaggia una squadra, ma la consapevolezza che senza il campo non c'è la partita. La collaborazione non è delega agli 'altri', è la modalità in cui il nostro singolo agire positivo si amplifica grazie alle moltiplicazioni dei nostri interlocutori. Il nostro impegno individuale non cessa nei sistemi collaborativi, ma resta al centro dell'equazione.

La sicurezza ha bisogno di regole, ma scompare di fronte al formalismo e non esiste dove la burocrazia ha il predominio perché si è persa di vista la missione: difendere la vita dell'azienda. Le norme servono per facilitare l'espletamento dei controlli, per impedire che una dimenticanza ci esponga a rischi, per assicurare che ciò che sappiamo rispetto al passato divenga esperienza condivisa.

La collaborazione diventa il fattore abilitante anche della applicazione di regole che, se sono condivise e comprese, sono controllate nella loro applicazione, non tanto dall'entità superiore di controllo, ma dall'insieme dei partecipanti.

Le regole non garantiscono l'immunità – come abbiamo visto esiste ciò che non sappiamo e che non esiste nelle regole – ma aiutano a ridurre il rischio e occorre in molti casi darsi regole ben

più severe di quelle previste dalle leggi, così come nei sistemi di qualità dobbiamo puntare a fare meglio di ciò che ci siamo posti; perché l'atleta che punta a saltare esattamente quanto aveva fatto la volta precedente, quasi certamente non supererà l'asta.

Può essere utopico immaginare una rete totalmente sicura e protetta con utenti rispettosi quando il mondo reale sembra invece sempre più violento e prevaricatore. La rete, è importante ribadirlo, tende a rispecchiare il mondo esterno perché è lo specchio di quello che noi siamo. Ci offre però una grande opportunità, quella di creare mondi, di creare spazi tutelati per i nostri figli e aree di libertà anche quando queste non sono possibili nel mondo reale. È un grande sistema che può contribuire sensibilmente alla qualità della nostra vita e per questo va protetto e difeso.