Quaderni dell'Osservatorio eHealth e-Sanit@

1 2015

Ambienti Digitali

Democrazia e Identità digitale tra Libertà e Tutela del cittadino

Atti dell'incontro Roma 12 Dicembre 2014

e-Sanit@
Management dell'e-Healthcare

Demonizzato e scomunicato. La battaglia tra luce e oscurità.
San Mercurio uccide l'Imperatore Giuliano l'Apostata.
(Icona, Il Cairo - Chiesa di Bet Mercurios, Lalibela, Etiopia)

Quaderni dell'Osservatorio eHealth e-Sanit@

Introduzione

Parlare di ambienti digitali, di democrazia e identità digitale è argomento arduo per la difficoltà concettuale di inquadrare entro schemi e modalità riconoscibili un mondo liquido e sfuggente ormai nei suoi confini.
Liquidità è il termine utilizzato da Baumann per indicare proprio la contemporaneità postmoderna, che ha perduto ogni criterio di rigidità e perciò di identificazione. Un mondo, in cui a mancare è la stessa possibilità di "società", ovvero di gruppo fondato su una concreta condivisione di valori e di interessi. Ci avviamo, dietro la spinta della società dei consumi e delle tecnologie digitali, verso mondi plurimi, che non a caso stanno mettendo a dura prova gli assetti organizzativi delle stesse istituzioni.
Uno scenario all'interno del quale il ruolo giocato dalle tecnologie digitali è centrale. Motore stesso del mutamento, incontrollato, senza confini, espansivo, vettore di nuove forme di aggregazione
sociali e, perchè no, di nuove e molteplici identità. Il web è diventato il luogo, in cui si affaccia una nuova umanità, dai tratti ancora incerti, ma che sta avviandosi a costruire mondi paralleli, alternativi e a volte contrapposti allo stesso mondo della realtà.
La stessa parola web (abbreviazione di world wide web 'ragnatela mondiale') rappresenta di per sé un mondo invisibile privo di sfericità o di mappe geografiche che ne possano dare informazioni di geolocalizzazione e quindi di orientamento spaziale.
Certo, gli ambienti digitali hanno ancora bisogno del mondo reale per nutrirsi, per attingere da esso le forme simboliche che in qualche modo li possano strutturare, ma è evidente che il tradizionale patrimonio simbolico e culturale stenta a fornire indirizzi e categorie di riferimento sufficienti.
Il dibattito di tutta la cultura occidentale si è giocato nel rapporto sottile, aspro, lacerante e doloroso, tra visibile e invisibile, tra realtà e trascendenza, tra oggetto e eidolon, tra apparenza e vero. Su questa riflessione e sui suoi risultati, si sono fondate e avanzate istituzioni, organizzazioni sociali, pensieri religosi e utopie.
L'ingresso del web ha, e sta allargando, questo dualismo, ne sta allontanando i poli magnetici, ponendosi come interlocutore terzo e promuovendo deragliamenti verso altri orizzonti, per noi ancora ignoti, le cui suggestioni sono le visioni di tanti autori di fantascienza e iperrealtà della letteratura americana ed europea di questo ultimo secolo.
E il web è anche il luogo di una frattura generazionale, quella che vede protagonisti i nativi digitali, giovani e giovanissimi, ragazzi e ragazze, nuova 'specie' imprintata sulla tecnologia e con essa strettamente interfacciata.
Internauta, hacker, cyber, nuove parole rimandano ad una realtà altra, forse irraggiungibile e incomprensibile per l'homo faber nato dalla pietra levalloisiana.
La potenza del web, pur in questo momento di contaminazione tra realtà e virtualità, è tale che alcune delle attività fondamentali dell'uno si stanno trasferendo nell'altro e che le scelte e gli avvenimenti del secondo hanno influenze incisive sul primo.
Uno stato di cose, che sta scuotendo le categorie stesse di diritto, di democrazia, di cittadinanza.
E' evidente che il mondo virtuale del web ha bisogno di un proprio statuto giuridico, ma gli attuali apparati giuridici ritardano nel varo di un codice internazionale, che ne regoli i territori, e affila l'unica arma che possiede per contrastarne il carattere anarchico e autocreativo, quella della tutela della privacy, della difesa della persona come soggetto di diritto nella sua intimità di pensiero e di emozioni.
L'identità disegnata dal Codice napoleonico con i suoi riferimenti civili, sostenuti dagli archivi anagrafici, che postulava la corrispondenza assoluta tra nome e stato civile, nel web si misura, ora, con identità plurime, nascoste dietro i nickname, certificate da anagrafi digitali anche fuori dal controllo delle stesse legislazioni statali.
La scommessa dell'identità digitale è quella di garantire un nuovo rapporto tra cittadino e identità in modo univoco, ma la sua regolamentazione giuridica si ferma dinanzi ai confini dei singoli stati e oltre diventa incontrollata.
Se sul nesso inscidibile tra cittadino e identità si regge il cuore stesso della democrazia e del suo ordinamento (un cittadino, un'identità, un voto), che ordinamento democratico avremo a fronte di plurime cittadinanze digitali?
Inoltre, le democrazie moderne, hanno fondato il proprio consenso sulla capacità di tutelare la persona in tutti i suoi aspetti, pubblici e privati.

e-Sanit@
Management dell'e-Healthcare

I temi della sicurezza e della inviolabilità della persona ricorrono nelle carte costituzionali, ispirano le leggi.
Che dire di fronte alla possibilità, per nulla remota, di minacce che giungono dal furto dei nostri dati, della nostra stessa identità, da attacchi indirizzati ai nostri sistemi, da manipolazioni frequenti delle coscienze, soprattutto quelle dei più giovani?
Domande, a nostro avviso, per nulla secondarie o oziose, e che pongono delle urgenze. La prima tra queste è quella di accettare che al mondo della nostra 'realtà' si sta affiancando in modo sempre più pervasivo, irruente e silenzioso, un altro mondo, quello del web, che deve essere approcciato senza sminuirne l'incidenza e la pressione sui nostri comportamenti e che quindi necessita di un governo, la cui stabiltà potrà forse nascere anche da una mediazione con il popolo globale del web.
Non sarà possibile mettere in campo una governance efficace senza approcciare nuove forme di pensiero, che vedano il superamento delle abitudini cognitive dell'homo faber, creatore della propria realtà, attore unico della propria identità e dominatore del mondo e della tecnologia tradizionali. Non a caso, una nuova antropologia sta sorgendo sulle ceneri di quella avviata con entusiasmo nei primi anni del '900.
La tecnologia, che sostiene l'intero perimetro (se mai esiste un perimetro) del web, accresce le condizioni di benessere e felicità, ma non è governabile in modo univoco e unitario (basti pensare al tema degli standard). Vive delle stesse pulsazioni creative dei suoi abitanti, con modalità che la rendono instabile, sfuggente, incontrollabile. Ed è una tecnologia che sta avviando inediti percorsi cognitivi, che sta plasmando linguaggi e abitudini di pensiero e relazionali, riconfigurando l'intero universo culturale di riferimento.
Governare tutto ciò richiede il riconoscimento di nuovi spazi sociali e professionali, come anche di nuove e fondamentali competenze. E non solo per la ricerca di un linguaggio che sia il più condiviso possibile, ma per mantenere la giusta distanza, quella che garantisce a noi tutti empowerment e sicurezza.
È su queste riflessioni che nasce il primo **"Quaderno dell'Osservatorio e-Health e-Sanit@"**. Primo Quaderno, che raccoglie gli interventi di un incontro dedicato appunto ad "Ambienti digitali. Democrazia e Identità digitale tra libertà e tutela del cittadino", che si è tenuto lo scorso dicembre a Roma. Un appuntamernto, al quale sono stati chiamati relatori di varia provenienza e che hanno offerto il proprio punto di vista dai peculiari specula professionali.
Un'iniziativa pilota, questa del Quaderno, che vuole essere la prima di altre che la rivista e-Sanit@, Management dell'e-Healthcare, proporrà per il 2015.
Massimo Caruso
Direttore editoriale e-Sanit@

Nota
Le illustrazioni scelte per corredare il I Quaderno dell'Osservatorio e-Health e-Sanit@ sono state tratte dalla mostra intitolata "Social Media Heroes, Social Media Victims. From Hieroglyphs to Facebook", proposta da Laurent Chrzanovski, Archeologo e Antropologo, Centro Nazionale di Ricerca Scientifica di Parigi.

La mostra, la cui iconografia spazia dal II millennio a.c. ai nostri giorni, è stata pensata per sensibilizzare ad un uso responsabile del web, in particolare delle reti sociali. Per fare ciò, Laurent Chrzanovski si è servito di esempi storici noti per illustrare le modalità operative delle antichissime pratiche di elogio e di diffamazione "oggi di bruciante attualità, se consideriamo la crescita e i risultati spesso drammatici del cyberattacchi, condotti contro gli individui, le organizzazioni sociali e gli stati".

La mostra, ideata per conto del Ministero degli Affari Esteri della Romania per celebrare la nomina di Catalin Marinescu alla Presidenza del Consiglio dell'Unione Internazione delle Telecomunicazioni (UIT / ONU-Ginevra), è stata inaugurata nel giugno 2013 nel sedio globale dell'Istituzione. Presentata al pubblico per più di quattro mesi nel museo dell'UIT, e poi in Romania, ha richiamato più di 50'000 visitatori.
La mostra è comunque visibile online, in lingua inglese e francese, all'indirizzo: **http://swissacademy.eu/en/social-media-heroes-victims/**

Spunti storico-antropologici per comprendere l'uso frequente di abusi e reati nella società digitale

Laurent Chrzanovski, Antropologo Univ. di Losanna e del Centro Nazionale di Ricerca Scientifica, Parigi

Prologo

La società italiana si è rivelata negli ultimi trent'anni come una delle più "golose" in Europa per l'appetito di strumenti tecnologici. Un comportamento certamente legato anche al successo dell'industria pubblicitaria, che vanta nel Bel Paese un'ampia longevità. Basti solamente ricordare il famoso "Carosello", pioniere, già nel 1957, per l'importazione nel Vecchio Mondo di tecniche di mercato d'Oltreoceano. Nonostante, tuttavia, la sua "golosità", la società italiana è ancora, purtroppo, in ritardo, anche negligente, se vogliamo a volte ingenuo, nel rapporto con l'uso delle tecnologie digitali che si tratti di telefonini intelligenti, di tablet, di laptop o di PC.

Un aspetto "culturale", che limita il valore del "marchio di fabbrica" del Made in Italy, caratterizzato dall'apertura di spirito, dall'abilità creativa, dalla ricerca di nuovi sbocchi commerciali. Pensiamo a Marco Polo, a Cristoforo Colombo, alle mille piccole, medie e grandi opportunità di sviluppio create nei secoli da uomini e firme italiane: banchieri lombardi e fiorentini, marchi come San Pellegrino o Lavazza, per non parlare dei beni di lusso (profumi, autovetture, oggetti di design etc...).

Finora, la preoccupazione più grande sembra essere stata quella di difendersi dallo spionaggio industriale e dalla concorrenza sleale dei prodotti contraffatti, distogliendo così l'attenzione dai pericoli provenienti dall'universo digitale. Pericoli generati da attacchi, frutto di azioni ostili, tese ad alterare i valori di mercato e che trovano terreno fertile nelle reti social e nell'utilizzo improprio di informazioni messe a disposizione dagli utenti e dalle stesse aziende. Gli attacchi commerciali e quelli alla reputazione aziendale sono solo uno dei tanti e molteplici aspetti di rischio che il web può generare. Ben più gravi sono quelli indirizzati al furto di dati confidenziali, strategici o personali.

Il problema maggiore è che questi ultimi dati, se isolati dal contesto possono apparire innocui e referenziali, non lo sono affatto nei processi di manipolazione criminale che avvengono nel web ad opera di specialisti della disinformazione. Manipolazione che può risultare fatale sia per il singolo individuo che per un'azienda. Se l'individuo ha una propria capacità di resistenza alla diffamazione e al ricatto, più robusta o più debole a seconda della solidità del carattere, le aziende, se non professionalmente consigliate nei protocolli della sicurezza informatica e della "counter information" assistono generalmente in modo passivo alla propria "laminazione" sistematica da parte di avversari ostil e anonimi.

Le Rivoluzioni della comunicazione

Per comprendere gli aneddoti storici proposti da chi scrive, bisogna ricordare che l'Umanità ha conosciuto sei importanti rivoluzioni mediatiche o, più precisamente, dei processi di comunicazione.

Si tratta delle invenzioni del "Verbo", i.e. della lingua (Homo habilis, 2.8 - 1.5 milioni di anni a.c.), della scrittura/lettura (IV millennio a.c.), della stampa (VII secolo d.c. in Cina - 1450 in Europa con Gutenberg), del giornale (dai pionieri del Seicento alla diffusione mondiale nel primo Ottocento).

L'ultima fase è quella dell'irruenza invasiva e pervasiva delle invenzioni tecnologiche, tutte concentrate negli ultimi due secoli. Nel solo Ottocento, assistiamo a quattro invenzioni rivoluzionarie, che in pochi decenni conquisteranno il mondo: il telegrafo, il telefono, la registrazione sonora e quella fotografica. Queste ultime poi protagoniste per la nascita dellla cinematografia, prima muta e poi sonora.

Negli anni '20 si impone quella della radio, importantissima in quanto radice della "cultura dell'immediato". Un'invenzione risalente all'Ottocento, ma ritardata nella sua operatività dai conflitti regionali europei prima e dalla Prima guerra mondiale poi. Il secondo conflitto globale ritarda ulteriormente la rivoluzione "gemella", che inaugura una maggiore immediatezza con la realtà, fino alla diretta: la televisione. Radio e Televisione due rivoluzioni fondamentali per comprendere l'uomo contemporaneo che si avvia ad immergersi nella "cultura dell'immediato".

Terracotta, esclusione e calunnia.
Ostraka con iscrizioni in caratteri ieratici in inchiostro nero (Giza). Scrivendo il nome di un nemico su un coccio e poi rompendolo, si eliminava la sua anima, dannandola per sempre.
© Museum of Fine Art, Boston

Per comprendere pienamente il carattere invasivo e sovvertitore dell'impatto delle tecnologie della comunicazione nelle abitudini mentali, sociologiche delle quattro ultime rivoluzioni, avvenute nello spazio di una generazione, più esattamente per l'Italia, in quattordici anni (1985-1999), è necessario mutare l'aspporccio antropologico abituale e codificato e avventurarsi nei terreni dell'antropologia digitale, sfuggenti e indeterminati.

Un approccio tanto più necessario da quando il ciclo delle rivoluzioni digitali culmina nel 1999, con la nascita dell'IoT (Internet of Things) presso il Massachussetts Institute of Technology.

Bisogna sottolineare che le tecnologie digitali, non sono in se stesse né buone né malvage, anche se, prive di governo, possono costituire una minaccia per la sicurezza e la tutela degli individui.

Che fare allora?

Di fronte a un insieme di problematiche così nuove, multiformi, dense di provocazioni sociali e giuridiche, è doveroso avvertire come il repentino cambio di marcia imposto dalle tecnologie digitali possa generare smarrimento dinanzi ad abitudini consolidate di approccio alla realtà.

Chi scrive, ad esempio, così come l'enorme maggioranza degli utenti, ma soprattutto dei decisori, a qualunque istituzione appartengano e qualunque ruolo svolgano, è spinto a riconoscere che è nato con la macchina da scrivere e con la televisione in bianco e nero, che lasciavamo il telefono uscendo dall'ufficio, che ricevevamo le lettere per posta e le notizie urgentissime via fax.

Di fronte al digitale che avanza, dobbiamo accettare umilmente di "ritornare a scuola" e riuscire ad adattarci "forzatamente", da adulti, a far fronte a problematiche che non ci sono assolutamente consone.

Sicuramente, le generazioni nate in questo secolo, le native digitali, saranno di gran lunga più a loro agio con il mondo virtuale di quanto lo possiamo essere noi. E saranno anche attori di nuove risposte in una società coerente con il prorpio universo antropologico.

Ma non possiamo testimoniare ogni giorni, per chi come noi non appartiene alla generazione natiuva, quanto ampia sia la distanza che ci separa, viepiù di giorno in giorno, dal mondo nel quale siamo nati, dai suoi valori

e siamo spinti a interloquire con ambienti cui non siamo stati preparati nè per i quali siamo stati formati.
Ci resta il senso della tradizione, del legame con il passato che forse può rappresentare un vantaggio sulle nuove generazioni. Ma bisogna saperlo declinare con i nuovi bosogni e nei nuovi contesti.

La tutela del cittadino nel contesto giuridico globale attuale
Il maggiore mutamento che rappresenta la profonda differenza tra la realtà attuale e quella di un'era finita ormai vent'anni fa non è tanto tecnologica quanto giuridica.
La difficoltà degli Stati europei di tutelare in modo efficace i cittadini proprio nelle loro relazioni con il mondo virtuale sta nella lentezza e nella eterogeneità delle proprie norme sul diritto di Internet e, soprattutto, sulla esecutività di azioni che vadano a contrastare con severità i reati che si consumano all'internmo della realtà virtuale, dai più elementari come la calunnia, la diffamazione, il ricatto, l'ostracismo, alla maniolazione psicologica, al furto di dati riservati e della propria identità).
Per dare risposte efficaci, considerando il carattere anonimo ed extraterritoriale degli autori di tali reati, è impportante avviare tra gli Stati forme di dialogo cooperativo, costruttivo e reciproco in materia di scambio di informazioni, soprattutto con quei Paesi che considerano la libertà d'espressione come un assioma inalienabile del proprio modus vivendi. UN problema aperto ad esempio resta quello della nazionalità dei server che registrano i dati cloud di utenti domiciliati ormai in qualunque parte del globo.
Negli ultimi mesi, ad esempio, due corti americane hanno condannato Microsoft a consegnare alla giustizia tutti i dati appartenenti ad un cittadino americano, ma stoccati in un server gestito nella sede irlandese della multinazionale. Se la Corte suprema confermasse il verdetto, vorrà dire che tutti i server di una compagnia americana, ovunque si trovino fisicamente come anche i loro contenuti rispondono unicamente alla legislazione statunitense.

Internet, Reti social e tecniche di esclusione
Nell'Atene cvlssica si usava un piccolo coccio (ostrakon) sul quale l'elettore incideva il nome del candidato. Gli ostraka venivano anche utilizzati per le decisioni strategiche rimesse al voto popolare, per i semplici inventari contabili e per il potere coercitivo: quello di condannare un cittadino a 10 anni di esilio (ostracismo).
Nel mondo moderno, l'ostracismo, nella declinazione in psicologia sociale e in sociologia, significa più ampiamente l'esclusione di qualcuno dalla società, da un gruppo sociale o da una comunità: si evita di comunicare con la persona ostracizzata o, addirittura, di notarla.
Il problema che si pone oggi, ai tempi di Internet, è che l'ostracismo, attraverso le reti sociali, è in grado di colpire ognuno di noi. Per escludere realmente un individuo dal suo gruppo sociale, bastano ormai, come ostraka, un numero cospicuo di "like" su un messaggio di cyberbullismo o di cyberstalking.
Le conseguenze psicologiche e sociali sono gravissime. E ancora una volta non si riesce a perseguire puntualmente chi compie tali reati, nonostante esistano modelli legislativi avanzati come il Codice della Privacy (D.Lgs 196 del 2003) italiano. Infatti, pochi sono i cyberbulli che sono stati indivduati e condannati. Merito la loro imprudenza, che li ha fatti agire senza precauzione, come quelle di utilizzare un falso indirizzo IP, un computer pubblico (universitario, etc...), ed uno pseudonimo.
In molti altri casi, l'Autroità di Polizia non è in grado di risalire facilmente al colpevole, spesso individuato dopo un lungo e analitico lavoro e soprattutto attraverso l'assistenza delle autorità di tutela internazionali. Ma la capacità di risalire al cybercriminale dipende soprattutto dalla disponibilità dei provider di rete a collaborare o meno.
E' palese la debolezza inammissibile della Commissione Europea nelle negoziazioni recentemente concluse con Google, che dà alla parte lesa la possibilità di eliminare dal motore di ricerca messaggi offensivi nei confronti della sua persona per difendere dunque la sua reputazione , ma solo sulle interfacce nazionali di Google con domiciliazioni nei 28 paesi dell'UE e dei paesi della zona Schengen come la Svizzera, la Norvegia e l'Islanda. Basta cercare il nome della "vittima" su un'altra interfaccia (.us, .com, .mx etc...) e nulla è cambiato.

Il dilemma politico di principio per lo spazio digitale
Quale libertà sarà consentità, nem mondo digitale, al cittadino digitale?
Le grandi potenze (USA, Russia, Cina) hanno scelto azioni interventiste, anche al punto di violare la privacy stessa dei cittadini, gestendo e/o censurando massicciamente le reti sociali ed i motori di ricerca, come anche altri paesi come l'Iran (Rete Cloob) e i Paesi dell'Asia centrale (Rete Odnoklassniki).
Negli stati della UE c'è invece più tolleranza, legata anche alla diversa percezione della pericolosità del probelm,a legato alla cybersecurity.
Ma di fatto, credere che la tutela della privacy, nel mondo digitale sdia difesa, è illusorio. Forse non è mai esistita oppure è diventata nel mondo digitale uno tra i beni più costosi.
Rimane un problema sottovalutato e insufficientemente affrontato per negligenza politica e incertezza esecutiva alle provocazioni che provengono dal web.
Per illustrare questa ipotesi, daremo due esempi recenti tratti dall'attualità politica e sociale romena. Il primo è quello della controversia, che dura da ormai dieci anni, sullo sfruttamento del bacino aurifero della zona di Rosia Montana.
La battaglia mediatica e digitale oppone la Rosia Montana Gold Corporation (RMGC, filiale della multinazionale canadese Gabriel Resources), che vinse la gara d'appalto, ma che non ha ricevuto il nullaosta dello Stato per l'inizio delle attività, a una nebulosa di attivisti molto ben organizzati e ormai apertamente sponsorizzati da una marca di acqua minerale, che non è altro che la ditta acquisita nel 2003 dal primo produttore mondiale di bibite gasate.
Recentemente, ad opera di hackers performanti, gli oppositori al progetto

La Gemma Augustea. Un Post del potere imperiale.
Cammeo in onice d'Arabia,
rappresentante Augusto accolto dagli dei e ammesso nel loro cenacolo come pari.
Sul registro inferiore, soldati erigono un trofeo in memoria delle vittorie dell'Imperatore.
© Kunsthistorisches Museum, Wien

hanno diffuso alla stampa, tramite le reti sociali, le tabelle contabili con i dati confidenziali dei compensi accordati dalla Gold Corporation a un cospicuo numero di universitari e di accademici (storici, archeologi, biologi etc...) per i loro contributi editoriali e interventi pubblici all'interno del "Gruppo independente per la monitorizzazione del patrimonio culturale di Rosia Montana". Il risultato è stata la più grande manifestazione della Romania post-comunista – complice le reti cocial - (più di centomila persone nelle strade delle principali città del Paese, un terzo a Bucarest, il 16 settembre 2013).
La giustizia non è riuscita fino ad ora a raccogliere adeguati indizi probatori sull'identità dei cybercriminali, che sono riusciti a rubare la lista delle "buste paga" della RMGC.
L'ultimo esempio di attacco con volontà destabilizzante è stato quello della messa in rete, in piena campagna presidenziale romena, su un sito creato appositamente in Ukraina e lasciato "aperto" solo mezz'ora (il tempo necessario ai media romeni di scaricare il materiale pubblicato), di fotografie compromettenti. 62 istantanee, che mostravano il Procuratore capo della Direzione di contrasto al terrorismo e alla criminalità organizzata (DIICOT), ex direttrice della Compagnia nazionale di Investimenti e, soprattutto, leader del partito del "Movimento Popolare", infine pupilla dell'attuale Presidente della Repubblica e candidata alla futura presidenza. Le fotografie, scattate nel marzo scorso a Parigi, sono state affiancate alle copie di spese esorbitanti effettuate in negozi della capitale francese e nell'albergo di lusso, dove ha soggiornato.
La notizia gettata in un contesto di tensione interna, ha ulterioremente accentuato la rapidità con cui il Procuratore è stato condotto al carcerde preventivo, per una precedente indagine di concussione sul suo conto.
L'identità delle persone coinvolte nella diffusione delle fotoe edelle ricevute di spesa, nella creazione dell'effimero blog ucraino e della sua pubblicazione nel web sarà ardua, se non impossibile.

Conclusione
Concludo richiamandomi ad un esempio noto a tutti voi sicuramente e adattato al mondo digitale Mariana Net, ha proposto una versione Di Romeo e Giulietta di Shakespeare adattata all'era multimediale ("Romeo, Giulietta et l'ordinateur", in L. Chrzanovski (ed.) Des premières écritures au Mutimédia. Une brève histoire des communications et bien plus..., Alba Iulia (Altip), 2010).
Frate Lorenzo manda un e-mail a Romeo, a Mantova, ma Frate Giovanni, specialista in websecurity, constata che l'e-mail è stata piratata e che il testo digitale non è mai giunto al destinatario.
Ma accade di peggio. Il contenuto del mail viene utilizzato contro i Francescani da una comunità evangelista del Texas, che lo riprende e lo inserisce su Facebook e Twitter, scatenando una propaganda mondiale antivaticana. Il suicidio di Romeo, immediatamente seguito a quello di Giulietta, filmati prodotta da una webcam nascosta, vengono diffusi in diretta sulla rete da un sito web scandalistico, domiciliato alle Isole Turks and Caiman.
Le azioni dei Montecchi e dei Capuleti crollano e, dopo un'OPA ostile, le due "aziende" sono acquistate integralmente da una multinazionale cinese. Escalo, sindaco di Verona, chiede al Procuratore della Repubblica di fare luce sul gravissimo danno arrecato all'economia della città, nonché ad un ordine religioso molto stimato e autorevole.
Ormai sul lastrico, le famiglie Montecchi e Capuleti sporgpono una prima denuncia penale per omicidio colposo e una seconda per manipolazione di dati per creare le condizioni dell'OPA ostile. Un'anno dopo, non avendo ricevuto nessun appoggio, nonostante l'aiuto di Interpol, tutti i casi vengono chiusi senza colpevoli.
Il gruppo criminale responsabile del furto dei dati dal server mail di Romeo non è stato identificato. Dopo le testimonianze della comunità evangelista texana, che ha negato categoricamente che i suoi social media officers

Ivan IV (1530-1584). Identità multiple
Un modo di rendere al pubblico
l'immagine complessa di uno zar dalla personalità complessa.
I profili di Vlad in Sergej Eisenstein (Locandina)

fossero all'origine dei messaggi Twitter e Facebook, i tribunali distrettuali di San Francisco e di San Matteo (California) hanno rifiutato di intimare a Twitter e Facebook, domiciliate sui loro territori, di rendere pubbliche le IP dei computer utilizzati per scrivere e mettere in rete i messaggi.
Infine, considerando l'assenza di un trattato giuridico di reciproca assistenza con l'Italia, la Corte di Cassazione delle Turks and Caiman ha rifiutato di compiere un'inchiesta sul sito che aveva consegnato alla rete il duplice suicidio di Romeo e di Giulietta.
In assenza di prove, il Tribunale Amministrativo di Pechino ha sollevato la multinazionale cinese da ogni accusa di manipolazione dei dati sensibili per creare le condizioni di un'OPA ostile.
Fuor di metafora, un invito a comprendere il "linguaggio", l'alfabeto, la chiave di lettura del mondo digitale, per non diventare, come scriveva Roland Barthes, ".....dei Dominicì in potenza, non assassini, ma accusati privati di linguaggio, o peggio camuffati, umiliati, condannati sotto quello dei nostri accusatori. Rubare il linguaggio a un uomo proprio in nome del linguaggio, tutti gli assassinii legali cominciano da qui" (Roland Barthes, Miti d'oggi, edizione italiana a cura di L. Lonzi, Torino (Einaudi) 1974, p. 44).

Ambienti Digitali e responsabilità: il connubio indissolubile

Luigi Zampetti, Marketing Business Telecom Italia

Se volessimo indicare la cifra del periodo storico che stiamo attraversando, probabilmente dovremmo scegliere "Internet", la rete mondiale di inter-connessione tra reti di computer, cresciuta nella prima metà degli anni '90.
Con il World Wide Web si è andata gonfiando, negli ultimi anni, un'onda di innovazioni che crea una forte discontinuità con il passato: la diffusione impetuosa della rete mobile, la pervasività dei Social Network, il paradigma del Cloud Computing, e poi Big e Open Data, l'Internet of Things stanno modificando profondamente abitudini e comportamenti.
Interi settori produttivi (intrattenimento, musica, libri, hi-fi, fotografia, vacanze) sono in via di ristrutturazione, altri (sviluppo delle APP, erogazione di nuovi servizi, ecc) nascono o si espandono. Tutti devono rimodellarsi per la possibilità di comparazione dell'offerta, per la maggiore prossimità del cliente, con le analisi delle opinioni social, etc...
Le istituzioni e perfino le forze dell'ordine devono fare i conti con aspettative e con possibilità finora inesistenti: la trasparenza attraverso la pubblicizzazione delle informazioni, la partecipazione alle scelte, l'organizzazione di manifestazioni tra gruppi chiusi, la geo-localizzazione dei sospetti, la rilevazione delle opinioni sui social.
Le persone, soprattutto le nuove generazioni, condividendo la propria vita sociale ed anche una larga parte della propria intimità (foto, rete amicale, storia personale, opinioni, preferenze, credenze), rischiano di ridurre il perimetro della propria identità, che dovrebbe restare inaccessibile, andando incontro a nuovi pericoli, a nuove fragilità. Di più: la possibilità di avere a disposizione, in qualunque momento, le informazioni di cui si ha bisogno, e di poter entrare o restare in contatto con gli altri, crea un senso di onnipotenza, che però si concretizza – miseramente - nelle capacità del device e della rete di connessione, con immancabili frustrazioni per la parziale o momentanea inadeguatezza delle tecnologie.
Ancora: se il (mio) mondo è il device, e posso portarlo con me, allora non posso più farne a meno, ma posso fare a meno di rendere fisici i miei rapporti. In conclusione, c'è la sensazione che le azioni reali ed i fatti virtuali abbiano la stessa consistenza, lo stesso peso, ed ai termini "inviolabilità, integrità, cancellazione" tipici delle tecnologie si sono affiancati "privacy, reputazione, oblio" propri del mondo individuale.
Il neurologo e neurochirurgo Wilder Penfield (Spokane, Washington, 1891 - Montreal 1976) con i suoi studi, poi integrati dal neuroscienziato Giacomo Rizzolatti, ha rappresentato (1950) le diverse parti del corpo sulla corteccia sensoriale primaria: la figura umana, che ne risulta, è sproporzionata e grottesca (homunculus), perché le parti del corpo sono ingrandite in proporzione al numero di recettori cutanei in esse presenti.
Per questo, le mani, i piedi, la bocca sono enormi in confronto alla schiena, le gambe, l'addome.
Ebbene, sono in corso studi tesi a dimostrare l'impatto dell'uso dei nuovi device sul cervello, che nelle generazione digital native si trasforma in un ingrandimento della rappresentazione del pollice, proprio il dito più utilizzato con il touch screen. L'osmosi e la sovrapposizione tra i due mondi (reale e virtuale) sembrano trovare così una prima conferma scientifica, oltre che esperienziale.
Come sempre, saranno gli strumenti culturali la difesa più efficace, per capire limitando gli irrinunciabili danni che l'innovazione porta con sé, ma sfruttando fino in fondo le possibilità offerte.

Ambienti Digitali

In letteratura, sono "spazi immateriali" realizzati e accessibili con le tecnologie ICT, che rappresentano il risultato del bisogno di simulare il mondo, ricreandolo e dando la centralità a chi ne fa esperienza. Quindi è un concetto molto vicino alla multimedialità, la creatività, l'intrattenimento, l'apprendimento, la formazione.
Qui riprendendo lo stimolo dell'incontro su "Democrazia e Identità Digitale tra Libertà e Tutela del Cittadini", che gli ambienti digitali siano anche gli spazi di vita digitale delle persone, procederemo ad analizzare sinteticamente quanto si può evincere dall'esperienza comune, concentrandoci sull'ambito pubblico, per poi giungere a delle conclusioni.
Iniziamo analizzando le tipologie di azioni, che le persone svolgono sul web nei diversi ruoli (Cittadino, Paziente, Utente, etc..).
Nella vita privata, accesso a siti web con log in, ai social network, ai servizi di entertainment, ad applicazioni di input/modifica dati, all'home banking, a personal mail; acquisti on line, giochi, scommesse.
Nella vita pubblica, accesso ad aree informative e servizi pubblici, a siti web con login, alla Intranet, alle Legacy Application, a web mail/PEC; firma di documenti/operazioni, upload di documenti firmati, pagamento di servizi, prestazioni, tasse, imposte.
Come si può facilmente rilevare; confrontando i due elenchi, esse stanno convergendo e il lato privato e pubblico sono sempre più sovrapponibili.
Proseguiamo analizzando alcuni emblematici casi di studio.
Un primario di telemedicina utilizza un social network commerciale per tenersi in contatto con i propri pazienti e la loro rete parentale, scambiando opinioni, suggerendo azioni, effettuando, ove possibile, diagnosi basate

Ivan IV (1530-1584).
Ivan IV sottomette il Kanato di Kazan. Piotr Korovin (1857-1919)

sulla condivisione di foto.
Un laboratorio di ricerca ICT ha realizzato un sistema di e-Voting, che rispetta tutti i criteri discriminanti (non coercibilità e trasparenza, sicurezza, segretezza, non ripudiabilità e validazione, equità, univocità e idoneità), basando l'identificazione del votante e la certificazione della volontà da esprimere sull'utilizzo delle nuove SIM NFC.
Un'azienda offre un enterprise social network per consentire ai pazienti, alla loro rete parentale, agli operatori socio-sanitari e alle strutture sanitarie di comunicare, informare, collaborare, condividere e dialogare.
Cosa si può osservare? Che i rapporti online tra soggetti sono sempre più plurali, quindi i processi sono meno soggetti al "governo" e sempre più alla "governance", cioè meno gerarchia e più condivisione.
Contestualizzando in ambito pubblico, si sta passando dall'e-Government alla e-Democracy, nella quale agiscono insieme i decisori istituzionali, i cittadini e le associazioni, per contribuire in modo propositivo, per fornire il feedback sull'erogazione dei servizi, per rendicontare sulla gestione, per dare trasparenza ai processi decisionali, per partecipazione alle procedure democratiche.
Tra l'altro, la e-Democracy è un tema studiato da 10 anni: nel febbraio del 2004 il Dipartimento della Funzione Pubblica insieme al Ministero Informatica Comunicazione dell'Università degli Studi di Milano e il DISPO (Dipartimento di Scienza della Politica e Sociologia dell'Università degli Studi di Firenze) di redigere le Linee Guida per la promozione della cittadinanza digitale.

Cosa ricavarne?

Che le nuove tecnologie sono la grande opportunità per coinvolgere erogatori ed utenti in modo innovativo, semplice, immediato; che la diffusione nella vita di tutti i giorni elimina alibi sull'adozione di queste tecnologie; che è la responsabilità, il principio per gestire tali innovazioni, declinato nel dominio del processo e nella certezza dell'identità.
Dominio del processo: la Netiquette si basa sulla autodisciplina dei singoli utenti di Internet dove, notoriamente, regna un'anarchia ordinata.
È sufficiente? Purtroppo no. L'utilizzo degli strumenti di condivisione quali social network, gruppi chiusi e aperti di discussione, blog, etc.., per garantirne l'uso corretto ed efficace a tutti, richiede che sia esercitata la moderazione e la censura. Sono ipotizzabili anche soluzioni di autogestione, come, ad esempio, l'obbligo da parte dell'utente-proprietario di assegnare una scadenza di pubblicazione a immagini, filmati, conversazioni che si intende condividere. In questo modo varrebbe il principio del "voglio essere ricordato", piuttosto del "voglio essere dimenticato".
Certezza dell'identità: secondo diverse rilevazioni (Rapporto OCSE, Contact lab European Digital behaviour study, CENSIS, GSMA), in media le persone hanno 26 login e solo 5 password, tendono a scriverle su carta o ricordarle a memoria (oltre un terzo), temono per il livello di riservatezza con cui sono trattati i propri dati personali (circa i due terzi), usano credenziali, che ritengono inaffidabili (oltre la metà). Tutto questo, nonostante siano continuamente oggetto di spamming e truffe, che dal 2005 ad oggi ci sono stati oltre 500 Mln di vittime di furti di identità.

Come uscirne?

Diffondendo (imponendo?) l'uso dell'identità digitale forte, che consentirebbe innanzitutto di avere sempre la certezza di chi agisce, e poi permetterebbe di fornire solo gli attributi commisurati all'azione: perché in qualunque circostanza dobbiamo comunicare il numero di telefono, l'indirizzo di posta elettronica, il domicilio fisico piuttosto che le proprie qualifiche?
D'altra parte, il quadro di riferimento è sempre più maturo: dallo standard ISO/IEC DIS 29115 - ITU-T Recommendation X.1254 sui livelli di sicurezza, al Regolamento europeo eIDAS n. 910/2014 23- lug-2014 sull'identificazione elettronica e i servizi fiduciari nel mercato interno, al progetto Stork2.0 per la realizzazione della «single European electronic

La forza delle parole. E' realtà?
Vladimir Il'ič Ul'janov arringa la folla. San Pietroburgo 1917

identification and authentication area», all'adozione di SAML2.0 come standard informatico de facto per lo scambio di dati di autenticazione e di autorizzazione.
In particolare, in Italia, sono attivi grandi "progetti di sistema": il Decreto Legge n. 179 del 18-ott-2012 (Crescita 2.0), così come modificato dalla Legge di conversione n. 221 del 17-dic-2012, apre al tema della «public digital identity management», definendo il Sistema Unificato di Identità Digitale a confluenza dei progetti di Documento Digitale Unificato (Carta Identità Elettronica, Tessera Sanitaria-Carta Nazionale Servizi), Anagrafe Nazionale Popolazione Residente (ANPR, AN Assistiti, AN Strade-Numeri Civici) e Domicilio Digitale (INI, Indice Nazionale Imprese e PEC, Posta Elettronica Certificata).
Il Sistema Pubblico di Identità Digitale (SPID) fungerà da «hub» per i diversi attori dell'ecosistema (Gestori dell'identità digitale, Fornitori di servizi, Gestori di attributi qualificati, Autorità di accreditamento e vigilanza), rendendo possibile la "interoperabilità delle identità digitali" rilasciate, ma previo accertamento de visu dell'identità fisica della persona.
Una grande spinta arriverà anche dall'espletamento della nuova gara CONSIP su servizi di cloud computing, sicurezza, realizzazione di portali e servizi online, cooperazione applicativa, che prevede l'acquisizione da parte delle Pubbliche Amministrazioni di servizi per la gestione delle identità digitali (Lotto 2, L2.S1-2-3). È in questo contesto che sul mercato si stanno affacciando soluzioni, in particolare su rete mobile, che consentirebbero di coniugare facilità, velocità d'uso, comodità, praticità, sicurezza.
Di quale tipologia? APP, quindi indipendenti dal sistema operativo del device e dall'operatore mobile scelto dall'utente; basate sulle SIM NFC, la nuova generazione di SIM card, che supporta la tecnologia NFC, dispone di un acceleratore crittografico RSA 2048, prevede la suddivisione in slot logico-fisici (Security Domain) per ospitare in totale sicurezza dati, applicazioni, certificati, chiavi anche di Service Provider/Terze Parti.
Non pensiamo che queste tecnologie servano solo per accedere in modo sicuro a siti internet o per firmare e cifrare documenti, ma anche per comprare e pagare ticket (metropolitana, musei, tram, parcheggi) piuttosto pagare gli acquisti in un negozio con il proprio cellulare, scaricare sul telefonino informazioni storiche e curiosità dai monumenti, mentre siamo in mobilità, sincronizzare rubriche o scambiare biglietti da visita tra due telefonini senza inviarsi SMS, come dimostrato a Milano nell'ottobre del 2012 durante l'NFC & Mobile Money Summit. In conclusione, la responsabilità è il requisito intrinseco all'agibilità degli spazi di vita pubblica digitale, requisito da rispettare e da fare rispettare, anche imponendolo, se si vuole che la Pubblica Amministrazione ed i suoi Utenti, noi tutti Cittadini, sfruttino la finestra di opportunità aperta dalle
tecnologie innovative.

Quaderni dell'Osservatorio eHealth e-Sanit@

e-Sanit@
Management dell'e-Healthcare

Legami oscuri tra Cybercrime ed Information Warfare. Democrazia digitale e controllo massivo nell'era post-Datagate

Raoul Chiesa, Founding Partner, President @ Security Brokers

Introduzione

Il 9 dicembre scorso, all'incontro "Ambienti digitali e democrazia digitale tra libertà e tutela del Cittadino", svoltosi a Roma ed organizzato dalla rivista e-Sanit@, Management dell'e-Healthcare, ho presentato un intervento relativo alla problematica del controllo massivo delle comunicazioni digitali.
Un tema sempre più attuale e urgente, soprattutto in seguito al c.d. "Scandalo Datagate", scoppiato in seguito alle rivelazioni dell'ex contractor dell'agenzia americana NSA (National Security Agency), Edward Snowden.
La presentazione nasce dall'esperienza mia e del mio team di ricerca sui temi del Cybercrime, del Digital Underground, dell'Hacking e della c.d. "Lawful Interception".
Negli ultimi quindici anni abbiamo analizzato l'evoluzione della cosiddetto «mondo hacker sommerso», che ha generato nuovi modelli di criminalità informatica e nuovi approcci, che si sono evoluti unitamente agli sviluppi dell'odierno mondo digitale e delle scelte effettuate dal mondo dell'Intelligence.
Proprio sulla base delle nostre ricerche e delle nostre esperienze sul campo nel contrasto a questi fenomeni, l'articolo accennerà al tema del Cybercrime nei suoi molteplici aspetti, analizzando l'evoluzione del c.d. "hacker's underground" e dei suoi attori, per sviscerare poi i modelli di business ed il modus operandi dei diversi protagonisti,
In conclusione, un'analisi puntuale della Democrazia Digitale e del Controllo Massivo delle informazioni nell'era Post-Snowden.

Sicurezza delle informazioni e reati digitali

L'approccio, che abbiamo portato avanti, ha avuto come punto di partenza il Cybercrime, in quanto fattore comune ed abilitante verso differenti scenari ed ecosistemi, tra cui il Cyber Espionage, l'Information Warfare e la c.d. "Lawful Interception", a sua volta un ecosistema che comprende le intercettazioni di tipo massivo.
Una prima domanda potrebbe, dunque, essere "perché è tutto cyber?". Le diverse risposte vedono infatti il Cyber Espionage e l'Information Warfare come protagonisti. Parliamo di tre minacce principali, in ordine di frequenza degli incidenti (ma non di gravità, nel qual caso l'ordine è inverso):
- Negligenza, errore umano e frodi realizzati da Insiders;
- Cybercrime transnazionale organizzato: incassa 15Md $ all'anno (2012), producendo danni diretti ed indiretti per quasi 400Md $ a livello globale;
- Cyber Espionage e Cyber Warfare, da parte di soggetti State-Sponsored e di mercenari.

Prima di addentrarci nel mondo del Cybercrime è però necessario fare un passo indietro.
L'affermazione, secondo cui "ogni nuova forma di tecnologia, apre la strada a nuove forme di criminalità", è purtroppo totalmente veritiera, concreta e sempre più attuale.
Il rapporto tra tecnologia e criminalità è stato, infatti, da sempre, caratterizzato da una sorta di "gara" tra buoni e cattivi.
Per esempio, agli inizi del '900, con l'avvento dell'automobile, i "cattivi" iniziarono a rubarle. La polizia, per contrastare il fenomeno, definì l'adozione obbligatoria delle targhe (car plates), ed i ladri iniziarono a rubare le targhe delle auto (o a falsificarle).
Nel XXI secolo, il nostro, potremmo dire che dalle automobili si è passati all'Information & Communication Technology (ICT) e che il concetto stesso di "rapina" è stato sostituito dal furto di informazioni.
Hai l'informazione, hai il potere (quantomeno, nella politica, nel mondo del business, nelle relazioni personali…) è certamente un'altra affermazione totalmente reale e, soprattutto, uno dei concetti principali del presente articolo.
L'affermazione, prima propugnasta, è però immediatamente trasformabile in:
- Vantaggio competitivo;
- Informazione sensibile/critica;
- Denaro;
- Ricatto.

Il collegamento può essere singolo (uno solo di questi punti) o multiplo, ovverossia uno o più punti che si sommano l'un l'altro.
Gli esempi su quanto affermiamo sono molteplici e c'è davvero l'imbarazzo della scelta, dalla Regione Lazio a Calciopoli, allo scandalo Telecom Italia/SISMI, all'attacco Vodafone Grecia fino a McLaren/Ferrari.
In tutti questi esempi, ma potremmo citarne un'intera moltitudine, lo scandalo è montato e le azioni criminose sono state compiute, perché alla base c'erano delle informazioni ed uno o più attori hanno trasformato questa conoscenza in un vantaggio competitivo o un'informazione sensibile (o critica), di cui erano a conoscenza (e dove non necessariamente la controparte era al corrente che terzi la conoscessero), o in denaro (per comprare il silenzio, o l'informazione stessa) o in un ricatto (che porta ovviamente del denaro in cambio del silenzio).

Il Cybercrime

Il concetto di Cybercrime si può definire come l'"utilizzo di strumenti informatici e di reti di telecomunicazione per l'esecuzione di reati e crimini di diversa natura".
Vi è un principio alla base della definizione e cioé "l'acquisire diversi insiemi di dati (informazione), tramutabili in denaro".
Il Cybercrime ha poi diversi punti salienti:
- Virtuale (modello "a piramide" ed anonimato, C&C, flessibili e scalabili, velocità di spostamento e rebuilding, utilizzo "cross" di prodotti e servizi in differenti scenari e modelli di business);
- Transnazionale;
- Multi-mercato (acquirenti);
- Diversificazione dei prodotti e dei servizi;
- Bassa "entry-fee";
- ROI (Return on Investment, per singola operazione, quindi esponenziale se industrializzato);
- Geografico e Geopolitico: paradisi fiscali e legislativi (cyber).

Sul fenomeno del Cybercrime, seppur di difficile quantificazione economica, diversi organismi istituzionali e isnternazionali (Nazioni Unite, Dipartimento della Giustizia USA, FBI, Europol, ENISA, Interpol) stimano, nel 2013, un fatturato di circa 20 miliardi di dollari, una cifra quasi doppia rispetto alle stime del 2011 (tra i 6 ed i 12 miliardi di dollari).
Parliamo del quarto crimine transnazionale al mondo, insieme al traffico di droga, di armi e di essere umani.
Se volessimo dare una ,visione "at a glance" di un tale fenomeno criminoso, potremmo descriverlo come "l'esecuzione di crimini, mediante l'ausilio di mezzi informatici e di telecomunicazione allo scopo di acquisire illegalmente informazioni e di tramutarle in denaro".
Il Cybercrime contempla diverse categorie di "servizi e prodotti", tra cui è certamente doveroso segnalare:
- Furto di Identità - info personali;
- Furto di Credit Identity - Informazioni finanziarie: login bancari, CC/CVV, «fullz», etc...;
- Hacking - verso e-commerce, e-banking, Credit Processing Centers;
- Industrial Espionage;

- Malware - Virus, Worm, Spyware, Key Loggers, Rogue AV, Botnets, Mobile;
- Hacking su commissione;
- Attacchi DdoS - Ricatto ("Blackmail"), Hacktivism
- Spam;
- Contraffazione - medicinali, prodotti di lusso nel campo della moda;
- Gambling - Riciclaggio di denaro - Finti siti e/o non autorizzati;
- Porno generico - Siti fasulli/civetta, etc...;
- Pornografia minorile / infantile.

Il Russian Business Network

Il Cybercrime si è evoluto e trasformato in un modello industriale 10 anni fa circa, intorno al 2004, quando vide la luce "RBN", il Russian Business Network, una gang del crimine organizzato, di stanza a San Pietroburgo.
RBN creò inizialmente un modello piramidale, internazionalmente distribuito, con un modello di business "win-win", accontentando tutti gli attori chiamati in causa e garantendo anonimato e privacy degli associati.
Un modello di marketing estremamente aggressivo, che diventò sin da subito il protagonista principale del crimine digitale su larga scala.
Un secondo, interessante aspetto. Che emerge dallo studio dell'approccio perseguito da RBN è stato quello della catena di comando e della "struttura di Governance", che vede hackers (cybercriminali), kingpins (i "cervelli" al capo dell'organizzazione criminosa) e gli e-launderers (riciclatori di denaro che utilizzano l'ICT), riuniti in un'unica entità, un unico gruppo organizzato, RBN appunto.
Alla base vi è l'Underground Economy, quell'economia sotterranea, che ha come scopo il commercio di beni ed informazioni rubate, di malware, di strumenti hardware e software, di capacità e di specializzazioni nel campo del crimine informatico.
E' tra il 2009 ed il 2010 che RBN "sparisce dai radar", con l'obiettivo di far credere alle Forze dell'Ordine ed ai ricercatori di sicurezza di avere chiuso i battenti. In realtà, l'organizzazione si disperde in tante realtà nuove e più piccole, meno visibili, quindi meno esposte: ad es. "IMU (innovative Marketing Ukraine), famosi per i loro finti antivirus e per un fatturato annuo di circa cento milioni di dollari, e Glavmed ed RX Promotions, noti per il commercio attraverso campagne di spam di prodotti medicinali contraffatti, tra cui Viagra e Cialis.

Il Cybercrime come "piattaforma di lancio" verso altri ecosistemi

Tornando al Cybercrime, parliamo di un ecosistema che è troppo spesso sottovalutato e che, nella maggioranza dei casi, è il punto di partenza o il transito verso altri ecosistemi:
- Spionaggio "classico", che utilizza gli skill ed il know-how propri del cybercrime odierno;
- Information Warfare;
- Black Ops (black operations);
- Cyber Espionage (industriale, governativo, militare, Intelligence);
- Hacktivismo;
- Cyber Milizie (private);
- Underground Economy e Black Markets;
- Crimine organizzato;
- Carders (frodatori di carte di credito);
- Gestori di Botnets;
- 0days;
- Malware factories (APT/Advanced Persistent Threats, outsourcing per la creazione di software maligni quali malware, etc...);
- Lupi solitari;
- "cyber"-mercenari, Deep Web, etc...

Iniziamo così a capire come il mondo dell'hacking e in generale gli "hackers", poco c'entrino con il Cybercrime, se non in casi specifici e particolari, e come l'odierno Cybercrime si basi su fattori ed aspetti abbastanza unici.

L'evoluzione dei diversi profili degli hackers e le rivelazioni di Edward Snowden

E' lo stesso mondo dell'hacking ad essersi evoluto negli ultimi venti anni, facendo sì che, oggi, sia davvero inutile, nonché sbagliato e superficiale, parlare in modo generico di "hacker".
Già nel 2004, chi scrive iniziò un progetto di ricerca internazionale all'interno dell'agenzia ONU "UNICRI" (United Nations Interregional Crime & Research Institute), chiamato "HPP", Hacker's Profiling Project.
Si trattava del più corposo progetto di ricerca mai eseguito al mondo verso il digital underground e la scena hacking internazionale, che ha portato all'identificazione di ben 9 differenti profili di "hackers", una classificazione, che ha fatto scuola e che, tra l'altro, è stata ufficializzata ed adottata nel nostro Paese dal DIS, l'Agenzia di intelligence nazionale.
Se c'era dunque nota l'esistenza di rapporti "particolari" tra il mondo dell'hacking ed i Governi ed i Ministeri della Difesa, non avevamo invece prove concrete in merito.
Quantomeno, sino a quando, nel 2010, un ex-contractor della NSA, Edward Snowden, non decise di scappare dalle isole Hawaii (dove lavorava in una base militare per conto dell'NSA come analista di Intelligence) e di recarsi ad Hong Kong e contattare giornalisti di inchiesta e testate note per la loro indipendenza e professionalità, facendo scoppiare il "caso Datagate", che ancor oggi interessa le pagine dei media mondiali.
Edward Snowden ha spiegato al mondo l'importanza dei c.d. "metadati", l'esistenza di programmi segreti di spionaggio globale, la violazione da parte del governo USA di diversi trattati e degli impegni di non spionaggio verso nazioni amiche (tra cui l'Italia, la Francia, il Belgio, la Germania).
Appaiono, allora, molto più chiari gli incidenti di spionaggio mirato, come il caso Vodafone Grecia, avvenuto tra il 2004 ed il 2005, nel quale circa 100 utenti "top" furono intercettati, sia nelle comunicazioni vocali che SMS: tra questi il Primo Ministro ellenico, il capo dell'Intelligence nazionale e altri diversi ministri.
Nel 2011 si venne a sapere che il budget della NSA per le c.d. "black operations" era pari a circa 650 milioni di dollari e che, a quella data, tali operazioni "sporche" erano state 231. Il caso greco è una di quelle operazioni, ma poco e nulla si sa delle altre 230!
Il 16 settembre 2013 l'operatore mobile del Belgio, Belgacom, denunciò la scoperta dell'esistenza di un sistema informatico di spionaggio ai danni dein propri utenti ed i cui responsabili erano, senza ombra di dubbio, la NSAn ed il GCHQ britannico.

Il problema del controllo massivo e della violazione imperterrita della privacy dei cittadini

Ricordo un bellissimo film, una co-produzione italo-tedesca, fortemente boicottato nei cinema nostrani, uscito nel 2006 e dal titolo "In Ascolto" (The Listening), nel quale il fornitore di una tecnologia speciale per le intercettazioni era arrivato ad avere più potere, decisionale ed esecutivo, che la stessa superagenzia di spionaggio sua cliente.
Un film lungimirante, nel quale la storia raccontata ricorda terribilmente proprio lo scandalo NSA, in diversi e molteplici aspetti, diversi anni prima che lo scandalo venisse a galla.
L'affaire NSA ci ha fatto comprendere come stia accadendo che i confini tra Cybercrime e Cyber Espionage siano sempre più labili, indefiniti e smarcati, ma anche come questi due ecosistemi siano ormai una parte totalmente integrante dell'Information Warfare.
Tali scenari non solo sono molto vicini a quanto prospettava George Orwell in "1984", ma hanno addirittura sorpassato quelle visioni di con-

trollo massivo delle informazioni nel più puro stile del "Grande Fratello". Durante la mia presentazione a Roma, ho ironicamente proposto la candidatura di Snowden al Premio Nobel per la pace, seguendo l'idea e la provocazione di diversi colleghi e personalità più o meno note, per le quali (incluso il sottoscritto) la NSA ha effettivamente esagerato ed ha superato quel confine invisibile che le Agenzie di Intelligence infrangono continuamente, senza farsi cogliere con le mani nel sacco, com'è invece accaduto.
La NSA, però, così come ogni altra Intelligence Agency del mondo, deve forzatamente avvalersi del supporto tecnologico di aziende private specializzate nel settore della c.d. "Lawful Interception", dello Spionaggio Elettronico, della censura Internet e del riconoscimento vocale automatico, tra cui troviamo diverse aziende italiane (Hacking Team, RESI/IPS, Area, etc...) e straniere (SS8, ZTE, Gamma, Vupen, Phoenexia, Ipoque, Blue Coat, etc..), alcune delle quali vendono i propri prodotti, nonostante affermino il contrario, a governi con regimi totalitari, dittatoriali ed oppressivi, quali Siria o Iran e, prima delle c.d. Primavere Arabe, Libia, Egitto e così via.

Un business globale in mano a pochi player, che intacca il principio stesso di democrazia

L'intercettazione massiva è, oggi, un business da ben 5 miliardi di dollari all'anno e vede protagoniste aziende private di 25 diverse nazioni. Un'industria segreta, di cui mal volentieri si parla.
Le tecnologie moderne di censura e di controllo massivo sono state altamente utilizzate durante le dimostrazioni in Venezuela ed in Ucraina, con scenari e comportamenti, che superano di molto le previsioni di Orwell e del suo "1984".
I Governi stanno abusando della tecnologia, con il sostegno delle aziende private e comportandosi come il Crimine Organizzato e come il Cybercrime. Un comportamento inaccettabile, un confine etico e morale, che è stato ampliamente superato e che creerà problemi sempre maggiori ed episodi di totale illegalità.
E' assolutamente necessario fare qualcosa e farlo subito, prima che sia troppo tardi. Concludendo il mio intervento a Roma ho riportato alcuni stralci del discorso tenuto da Mikko Hypponen, un esperto finlandese di sicurezza informatica, a "TED" nel corso del 2013, nella speranza che il mondo politico italiano ne prenda atto e coscienza, per evitare ulteriori futuri episodi, che sfuggono al doveroso controllo nonché necessario.
"Gli americani sono pronti a buttare via la Costituzione, buttarla nel cestino, solo perché ci sono i terroristi? La stessa cosa per il Bill of Rights (lla Carta dei Diritti) e tutti gli emendamenti, la Dichiarazione Universale dei Diritti dell'Uomo, le Convenzioni europee sui Diritti dell'Uomo e le Libertà fondamentali e la Libertà di stampa? Pensiamo veramente che il terrorismo sia una tale minaccia esistenziale da essere disposti a fare qualunque cosa?". La sorveglianza cambia la storia. Lo sappiamo da esempi di presidenti corrotti come Nixon. Immaginate se avesse avuto il tipo di strumenti di sorveglianza disponibili oggi. Fatemi citare testualmente il presidente del Brasile, la signora Dilma Roussef, uno degli obiettivi della sorveglianza della NSA. "Se non c'è nessun diritto alla privacy, non può esistere nessuna vera libertà di espressione e opinione, e quindi non può esistere una democrazia efficace. Ecco di cosa si tratta. La privacy è il mattone fondamentale delle nostre democrazie".
E per citare, infine,e un collega ricercatore nella sicurezza, Marcus Ranum, "gli Stati Uniti oggi stanno trattando Internet come se fosse una delle loro colonie. Siamo tornati all'epoca della colonizzazione, e noi, gli "stranieri", che usiamo Internet, dovremmo vedere gli Americani come i nostri padroni". Mikko Hypponen è stato il primo esperto di sicurezza informatica europeo a prendere pubblicamente posizione sullo scandalo NSA e, dopo di lui, in tanti lo hanno seguito.
Il mondo in cui viviamo oggi è drasticamente cambiato: è davvero il caso che ce ne accorgiamo! Ci fidiamo ancora "troppo" degli altri (free wifi, Google, Facebook, aziende dell'IT ed ICT, etc..) e non consideriamo il valore («oro») delle nostre informazioni.
La Comunità Europea è chiamata fare qualcosa e il Parlamento italiano anche, non possiamo più fare finta di niente. Le leggi, le normative e le regole di Ingaggio internazionali relative al mondo «cyber» vanno riviste, dato che, nonostante ciò che si dice e si scrive, quella "cosa che si chiama privacy» ce la siamo già giocata, molto, molto tempo fa.

Damnatio memoriae. Non è mai esistito.
La demolizione della colossale statua di Saddam Hussein.
Baghdad (9 Aprile 2003)

Come con la tecnocrazia l'individuo ha perso la propria centralità. Importante far cultura sui temi della Privacy

Graziano de' Petris, *Responsabile Ufficio Privacy nell'Azienda Ospedaliero-Universitaria "Ospedali Riuniti" di Trieste*

Il dato personale è un valore che appartiene strettamente agli individui e una società democratica non può permettersi di non tutelarlo, perché esso è parte essenziale del patrimonio soggettivo.
In sostanza il tema verte sul fatto che, in questa nostra società tecnocratica, l'individuo ha perso la propria centralità, perciò è importante far cultura sui temi della Privacy.
Permettetemi di citare Antonello Soro, paladino della difesa del nostro patrimonio informativo individuale, richiamando l'attenzione sull'importanza di quei valori, che si vanno eccessivamente affievolendo in questa epoca, nella quale assistiamo alla perdita dei mores maiorum, a fronte di sempre maggiori forme di discriminazione e di stigmatizzazione sociale, di larvata compressione dei diritti soggettivi e di strumentalizzazioni attuate da parte di chi vuole rendere la società democratica non uno spazio di libertà, ma un luogo di violenza e anomia, secondo una rinnovata logica totalitaria dell'uomo di vetro, applicata alla moderna società della conoscenza, della quale Internet è il pilastro fondante.
Vorrei richiamare l'attenzione su un particolare fenomeno. Il mondo virtuale degli Avatar, creato a partire dai primi anni novanta, che, grazie alla possibilità per chiunque, anche digiuno di tecnologie informatiche, offerta dalla creazione di quell'interfaccia grafica di navigazione multimediale semplice e intuitiva (browser web), permette a ognuno di simulare di essere chi non è. Relazionandosi giocosamente con altri non-loro virtuali, in un mondo non reale, che è divenuto però, parte integrante del vecchio mondo reale. In questo contesto, la comunicazione telematica ha assunto valore legalmente sostenibile e le azioni compiute dalle identità digitali hanno ora la stessa valenza di quelle compiute dalle persone fisiche. Ma non hanno la stessa dignità.

Come mai?
Alla nascita, ogni soggetto viene registrato all'anagrafe, al sistema sanitario, al sistema fiscale, etc... Assume cioè un'identità digitale. Ad ogni individuo viene poi data la possibilità di agire a distanza, in tempo reale, con tutti gli altri, annullando distanze e tempi di percorrenza, di compiere transazioni finanziarie senza recarsi ad uno sportello bancario, di prendere decisioni senza presentarsi fisicamente davanti ad un pubblico ufficiale. Di compiere, insomma, azioni anche a valenza legalmente sostenibile. Tutto qui.
Ma abbiamo avuto bisogno di inventare termini come identità digitale, mondo virtuale, avatar, perché abbiamo bisogno di classificare, di definire, di delimitare...perché abbiamo paura di ciò che non si vede. Abbiamo paura dell'ignoto e...abbiamo bisogno di certezze.
Tale fisiologica necessità di rimanere con i piedi per terra e di guardare dove si cammina, ha creato confusione, ha portato ad immaginare un altro noi, che agisce in un mondo invisibile, in qualche modo legato a noi, ma con un legame piuttosto labile.
Siamo pronti a disconoscerlo, se fa qualcosa che non ci piace, se si dovesse comportare male, quasi avesse vita propria. Si tende spontaneamente ad immaginare la nostra identità telematica come un burattino di cui si possono tirare i fili...per il momento. Ma in qualsiasi momento qualcun altro se ne può impossessare, facendogli fare ciò che vuole, perché il PC non fa ciò che vogliamo noi, fa ciò che gli si ordina da chi si presenta col nostro nome.

Un approccio errato
Non sono cambiate le regole del gioco, disponiamo soltanto di uno strumento in più per compiere, e subire, azioni a distanza, annullando lo spazio, e direi anche il tempo. Nient'altro che la naturale evoluzione di quello che ha fatto Guglielmo Marconi nel 1931, quando accese le luci della Statua del Cristo a Rio de Janeiro, premendo un tasto, standosene comodamente seduto in provincia di Pisa. Tutto qua.
Un bellissimo e potentissimo strumento, certo, ma solo di uno strumento si tratta. Abbiamo, invece, avuto bisogno di considerarlo una via di mezzo tra l'isola che non c'è e un'estensione di noi, come se ci fosse spuntato un terzo occhio, capace di vedere un mondo diverso dal nostro o un'antenna in cima al monte. Ci comportiamo come se stessimo esplorando questo nuovo mondo, questa nuova società ancora "primordiale", ancora da ordinare.
Alcuni si muovono in modo più prudente, altri meno. Alcuni sono spinti dalla curiosità dell'esploratore, altri dall'avidità del filibustiere.
Perché gli attori, sempre quelli, sono persone, buone o no, oneste o no, intelligenti o imbecilli. Tutti utenti (o "utonti", per usare un'espressione cara a Raoul Chiesa) della rete. Pescatori o pesci, tanto per rimanere in tema di reti.
La struttura legislativa, che ci siamo dati nel mondo reale, con l'intento di delimitare e di regolamentare gli ambiti di movimento e di azione di ognuno, all'interno di quella indispensabile libertà propria di ogni organismo democratico, mantenendo un sia pur delicato equilibrio per non interferire eccessivamente con la libertà altrui, è il frutto di millenni di evoluzione.
Mentre la previsione di fattispecie penali relative all'uso illecito e dannoso dei nuovi strumenti di comunicazione, che ci vengono messi a disposizione attraverso Internet (che è divenuta soltanto nel '91 quella che conosciamo e che tutti utilizziamo) si colloca, in Italia nel '93, con l'introduzione del reato informatico nel Codice Penale (Legge 547).
Uno spazio di tempo tropo breve è trascorso e troppi sono ancora gli angoli bui e le zone franche.
Bisogna comprendere che non sarà necessario attendere un millennio di evoluzione legislativa e giurisprudenziale. Bisogna comprendere, ora, prima che sia troppo tardi, che la rete non è un mondo nuovo a sé stante, popolato da nuovi individui, dove coloro che abitano il mondo reale cambiano veste, assumendo, nel loro agire virtuale, le fattezze di trogloditi digitali o di pirati con un occhio bendato e un rampino al posto di una mano o ancora di novelli conquistatori di un territorio abitato da popolazioni primordiali.
Ma ci rendiamo conto che le regole sociali in rete sono le stesse delle antiche tribù o dei clan, dove la vita stessa dell'individuo non aveva alcun valore, finché, attraverso il rito iniziatico, assumeva un ruolo utile al gruppo e la sua vita non valeva nulla, quando questo ruolo lo perdeva o gli veniva tolto? Perché è questo ciò che accade.
L'informatica applicata alla comunicazione e, in particolare, alle reti di telecomunicazioni, che hanno permesso la creazione della rete globale, non è nient'altro che uno strumento. La rete non è nient'altro che un potentissimo e fascincoso strumento e, come tutte le tecnologie potenti, la rete è, per sua natura, essenziale, ma anche pericolosa.
E sono bellissime le infinite possibilità che ci offre, solo a patto di utilizzarla con estrema attenzione e con le dovute cautele, perché diversamente potrebbe rivelarsi un'arma, dannosa per sé e per gli altri.
Dobbiamo fare, dunque, attenzione, perché, alla stessa stregua di un'arma, il suo uso non consente distrazioni. La potenza di questo strumento sta nella sua capacità di far progredire l'Umanità ad una velocità fino a qualche decennio fa assolutamente impensabile. Questa accelerazione, alla quale non siamo e non potevamo essere preparati, si sta rivelando, al contrario, uno strumento pericolosissimo, al pari e forse più di un'arma micidiale, perché il suo utilizzo incosciente o, peggio, malvagio, può essere causa di danni esistenziali, che nessuna pena o sanzione potrà mai essere in grado di ripagare, in particolare attraverso l'uso illecito o strumentale di dati sensi-

E' realtà?
Vladimir Il'ič Ul'janov si rivolge alle truppe (5 maggio 1920). Alla destra, in uniforme Lev Trotski. Alle spalle Lev Kamenev. Nel 1928, la censura cancella Trotski. Nel 1936 sarà il turno di Kamenev (ill. p. 10).

bili, come ad esempio di quelli relativi alla salute.
Ragionamenti come questi, sono alla base delle motivazioni che mi hanno spinto ad appassionarmi e ad occuparmi, ormai da un ventennio di tutela dei dati personali nella P.A.
E sono anche alla base delle motivazioni, che mi hanno spinto ad insistere per la costituzione di un laboratorio di ricerca sui temi della sicurezza informatica e della privacy in Sanità, che mi è stato affidato dall'Azienda Ospedaliero Universitaria di Trieste, della quale sono il Privacy Manager, o, più precisamente, il Chief Data Protection Officer.
L'eccesso di comunicazione compulsiva e incontrollata, associato alla mancata applicazione delle adeguate restrizioni di sicurezza sui dispositivi mobili, produce anche, e forse principalmente, l'effetto di arricchire chi detiene la possibilità, lecita o illecita che sia, di utilizzare a proprio vantaggio gli strumenti della comunicazione, non solo attraverso la veicolazione di pubblicità mirata e l'induzione di bisogni e aspettative, a spese di risorse e di tempo conferito inconsapevolmente e gratuitamente dagli utilizzatori, ma anche di utilizzare le informazioni stesse a scopo assolutamente fraudolento, potendo contemporaneamente disporre di un'inimmaginabile mole di informazioni da utilizzare o rivendere ad altri malfattori, in un effetto a cascata senza fine. E non voglio, qui, affrontare l'argomento del controllo delle masse o di intere nazioni, di cui si vanta tanto l'NSA. E non voglio neanche affrontare il tema della Cyber Warfare, che è in questo momento in pieno svolgimento a livello mondiale tra grandi e piccole potenze, sia sul piano economico che su quello militare. E non affronterò nemmeno il tema del terrorismo internazionale e della sua eccezionale capacità di utilizzare questi strumenti, che sono veramente quanto di meglio avrebbero mai potuto sperare di avere a disposizione. Gratuitamente.
Tutti questi aspetti richiederebbero approfondimenti peculiari e troppo estesi per il tempo che mi è stato assegnato.
L'elaborazione di questa enorme massa di informazioni liberamente disponibile in rete mediante l'utilizzo di strumenti sempre più potenti e sofisticati di ricerca semantica e aggregazione finemente mirata, resa possibile ormai anche sulle immagini fotografiche e sui filmati, sulla stessa voce e addirittura sulle abitudini di vita, sugli orientamenti politici e religiosi, sulle preferenze sessuali, sulle fobie di ciascun singolo individuo sui punti di forza e di debolezza del carattere di ognuno.
Tutte queste e molte altre informazioni, rilevate indirettamente anche attraverso sofisticati sistemi d'analisi delle abitudini e perfino del tempo impiegato da ogni soggetto su ciascun singolo dispositivo di comunicazione, suddiviso tra PC, tablet o smartphone; i profili psicologici soggettivi rilevati attraverso l'analisi d'uso degli strumenti di comunicazione sociale, per ciascun singolo individuo e, aggregando i dati, per ciascuna categoria, razza, appartenenza, etc... hanno fatto assumere ai sistemi di connessione e di comunicazione in rete il ruolo strategico di gangli nodali della società attuale, dov'è la comunicazione stessa a generare utile economico e a consentire il controllo puntuale della vita degli individui.
Per questo motivo la rete è estremamente strategica. Ecco, allora, perché la moderna guerra per l'egemonia economica sul mondo globalizzato si combatte in Internet.
Oggi, ci dicono che è cambiata l'era geologica, che l'uomo digitale non ha più privacy. Abbiamo visto come chi sia molto potente possa conoscere tutto di chiunque. Abbiamo sentito che una società che subisce una diffamazione mirata in rete, ha statisticamente soltanto sei mesi di speranza di vita senza un Social Officer a difendere la sua reputazione in caso di attacco da parte della concorrenza attraverso i media e che, più grande e ricca è, più è in pericolo.
Abbiamo sentito che in America il 19% degli adolescenti, che hanno subito cyber stalking, tenta il suicidio. Abbiamo potuto sentire degli sforzi del Garante per la Protezione dei dati personali, nel riuscire ad imporre un mutamento di atteggiamento ad un colosso come Google. Abbiamo compreso il significato pratico del concetto di diritto all'oblio, la grande difficoltà nel riuscire ad applicarlo efficacemente e il reale conflitto che c'è tra necessità di sicurezza e libertà. Abbiamo capito che siamo spinti a comunicare compulsivamente e che il "know me espectation" non è tanto un servizio utile, quanto un modo per indurci dei bisogni. Abbiamo visto che siamo in piena cyber war, in particolare economica.
Qualche tempo fa credevamo che il modo migliore per cancellarsi da un social network fosse quello di modificare prima tutti i dati personali con altri non riconducibili a sè e sostituire le informazioni presenti nel profilo con altre prese a caso, consapevoli che i dati rimangono comunque in possesso del gestore. Pia illusione.
Sappiamo che nemmeno questo ha più senso. L'eccesso di comunicazione e l'abuso della tecnologia assomigliano a un cane che si morde la coda, sono lo yin e lo yang dei tempi moderni.

C'è bisogno di consapevolezza

Solo la consapevolezza genera sicurezza e porta a comportamenti attenti e corretti, per sé e per gli altri. È quello di cui abbiamo tutti bisogno. Ed è su questi temi che bisogna aumentare il grado di consapevolezza, non soltanto dei singoli frequentatori del web, ma in particolare di coloro che sono delegati a compiere scelte che impattano su tutti.

Privacy e Data Protection. Le risposte all'esigenza di tutela vengono da più parti. La sinergia può lasciarci fiduciosi sul futuro

Luigi Montuori, Capo del Dipartimento Comunicazioni, Garante dei dati personali

Nel ringraziare gli organizzatori del convegno mi complimento innanzitutto per la scelta degli interventi che ho trovato sin qui di estremo interesse.
Mi sembra anzi doveroso invitare gli organizzatori a riproporre il tema in un nuova occasione di incontro per permettere la partecipazione a un numero sempre maggiore di persone interessate al tema della protezione dei dati personali nelle sue varie sfaccettature.
Il tema dell'identità digitale richiama inevitabilmente concetti come protezione dati personali, dignità, sicurezza, riservatezza.
Pochi anni fa è stata teorizzata da più parti la morte della privacy.
Ricordiamo Mark Zuckemberg di Facebook e Scott Mac Nealy di Sun Microsystem. Ma se analizziamo alcuni fatti accaduti nell'ultimo anno ci rendiamo conto che tali affermazioni possono essere smentite.
Ne ho in mente tre.
Il primo è dato dal clamore mediatico suscitato dalle rivelazioni di Edward Snowden. In tutto il mondo, Europa compresa.
Si sono sollevati interrogativi sulla legittimità ed anche sull'utilità di una indiscriminata sorveglianza di massa anche grazie all'utilizzo dei dati personali detenuti a vario titolo da società di telecomunicazioni e dai cosiddetti Over the top.
Il secondo punto, meritevole di attenzione, è offerto da alcune recenti pronunce della Corte di Giustizia della UE. Mi riferisco in particolare alla decisione dell'8 aprile 2014 in materia di data retention, che ha evidenziato l'esigenza di maggiori garanzie a tutela della protezione dei dati personali telefonici o telematici detenuti da fornitori di accesso alle reti conservati a fini di giustizia.
La Corte in questo caso ha invalidato la Direttiva Europea, che prevede come obbligo la conservazione di dati di traffico, ritenendo sproporzionata tale misura in assenza di idonee garanzie a tutela dei cittadini europei. Tale Direttiva è sicuramente molto importante, perché fissa criteri sui quali basare il bilanciamento tra le esigenze di sicurezza e quelle di protezione dei dati personali.
Altra recentissima sentenza del giudice lussemburghese è quella del 13 maggio scorso sull'oramai noto caso "Costeja Gonzales", che ha stabilito, da un lato, la competenza delle autorità nazionali sui trattamenti di dati personali effettuati da Google e, dall'altro, ha riconosciuto anche il diritto di chiedere, in prima battuta direttamente alla società americana, la cancellazione dei propri dati personali dai risultati ottenuti tramite il motore di ricerca. Entrambi gli aspetti affrontati dalla sentenza mettono finalmente fine a una lunga diatriba interpretativa tra autorità nazionali di controllo e Over the top.
Gli apprezzamenti e le critiche che ne sono scaturite fanno capire quanti "interessi" e quanto interesse sottostà a tale tema.
Le polemiche sul diritto all'oblio ne sono solo un aspetto ma, visto il titolo del convegno di oggi, diventano un punto centrale in tema di identità digitale. Il Professor Rodotà recentemente ha posto una domanda: siamo quello che riteniamo di essere o quello che la rete dice di noi?
Sicuramente avere la possibilità di chiedere di cancellare i propri dati dai risultati dei motori di ricerca aiuta a riappropriarci della nostra identità.
Analogamente quando una notizia che ci riguarda non è più attuale e non ha alcun interesse pubblico ad essere conosciuta, o è inesatto, non accurata, abbiamo il diritto a chiederne la deindicizzazione.
Anche in questo ambito va affrontato in modo corretto un bilanciamento. In questo caso tra protezione dei dati personali e identità personale da un lato e diritto alla manifestazione del pensiero e quello a conoscere, a essere informati dall'altro.
Il terzo punto è quello che riguarda i lavori in corso per un nuovo Regolamento europeo in materia di protezione dei dati personali.
La Commissione europea nel gennaio 2012 ha presentato al Parlamento e al Consiglio dell'UE il c.d. "pacchetto protezione dati", che contiene anche una proposta di Regolamento in materia di protezione dei dati personali, che dovrà prendere il posto della Direttiva del 1995, recepita in Italia, prima con la Legge 675/1996 e infine con il Codice Privacy del 2003.
L'Europa ha infatti avvertito la necessità non solo di aggiornare la disciplina del 1995, ma di migliorarla eliminando quegli obblighi, che l'esperienza ha dimostrato essere percepiti come di tipo formale-burocratico, inserendo invece attività orientate ad una maggiore consapevolezza dei cittadini interessati e responsabilizzazione dei rischi e dei danni collegati al rilascio e alla circolazione dei propri dati personali.
Lo strumento prescelto del Regolamento non è casuale, ma individuato appositamente onde risolvere o comunque limitare alcune disomogeneità applicative fra i vari Stati membri chiamati a recepire la Direttiva attualmente vigente.

I lavori, come prevedibile, sono stati accompagnati da un dibattito molto intenso, all'insegna di tesi e posizioni spesso fortemente confliggenti.
La materia è sicuramente complessa e gli interessi giuridici ed economici, contestualmente in gioco e da contemperare, sono assai rilevanti e riguardano non solo il settore privato, ma anche il settore pubblico.
La proposta del nuovo Regolamento ha subito nelle Commissioni parlamentari circa 4 mila emendamenti, realizzando un vero e proprio record nella storia del Parlamento europeo.
Nonostante tutto, però, la fase critica dei lavori parlamentari sembra essere stata superata, secondo alcuni anche grazie alla pressione mediatica causata dalle note rivelazioni di Snowden.

Se volessimo fare delle previsioni sul tempo di approvazione del nuovo regolamento, possiamo immaginare che il negoziato da parte del Consiglio UE possa avvenire nel primo semestre 2015.
Ciò porterebbe a definire il quadro complessivo delle misure di attuazione nel 2017 e, presumibilmente, la completa operatività dal 2020.
In attesa di questo nuovo quadro giuridico, le Data Protection Authority sono al lavoro. Per citare alcuni recenti interventi della nostra Autorità, posso indicare quello relativo agli aspetti di sicurezza, come le violazioni dei dati personali, cd.
Data breach, oppure in tema di profilazione in rete. Mi riferisco anche al provvedimento di maggio scorso sui cookie, in cui il Garante, dopo una consultazione pubblica, ha indicato modalità semplificate che consentono di informare gli utenti della rete e di chiedere il loro consenso per l'utilizzo di tali dati.
Provvedimento questo ritenuto innovativo e oggetto di studio e di attenzione da parte delle altre autorità europee e che entrerà in vigore dal giugno prossimo.
Un ultimo riferimento relativo al provvedimento del luglio scorso, con il quale il Garante, primo in Europa, ha prescritto a Google Inc. di adottare modalità che consentono di rispettare il Codice privacy per le attività in rete. Come si può vedere, sono temi in continua evoluzione, che pongono anche nuove criticità. L'interessante è notare come le risposte all'esigenza di tutela vengono da più parti: dal legislatore comunitario e nazionale, dalle varie Corti di giustizia e dalle autorità nazionali.
La sinergia di questi soggetti, unita all'attenzione che ognuno di noi deve fare nel momento in cui gestisce i propri dati personali, può comunque lasciarci fiduciosi sul futuro. La privacy non è morta anzi direi che vive una nuova giovinezza.

L'interrealtà. Quando la velocità del Web sollecita il cambiamento nell'educazione degli adolescenti

Corrado Lonati, Presidente Associazione Icaro ce l'ha fatta ONLUS

Da qualche mese è disponibile sul web un video (www.youtube.com\Iforgotmyphone), che riassume in due minuti tutti gli argomenti presentati e discussi in questo convegno.

L'idea è alla base del filmato molto semplice: come sarebbe la nostra giornata senza smartphone? Cosa riusciremmo a vedere se ci dimenticassimo a casa il cellulare? Il video risponde a queste domande attraverso gli occhi della protagonista: senza avere il collo incurvato verso lo schermo nero del telefono, osservando gli altri che hanno le nostre stesse abitudini, riusciremmo infatti a vedere quanto è bizzarro il nostro comportamento quotidiano. Gente che fa footing e si ferma al primo squillo per discutere lungamente al cellulare; gli amici in silenzio attorno al tavolo del bar che sì, comunicano chattando con persone lontane, ma non parlano con chi sta loro vicino; i compagni di squadra del bowling che non guardano il risultato del tuo tiro perché troppo impegnati a postare in tempo reale le loro foto; lo scrolling dei whatsapp a letto un po' come facevano una volta gli anziani con la sigaretta... l'ultima cosa prima di dormire, la prima cosa dopo essersi svegliati.

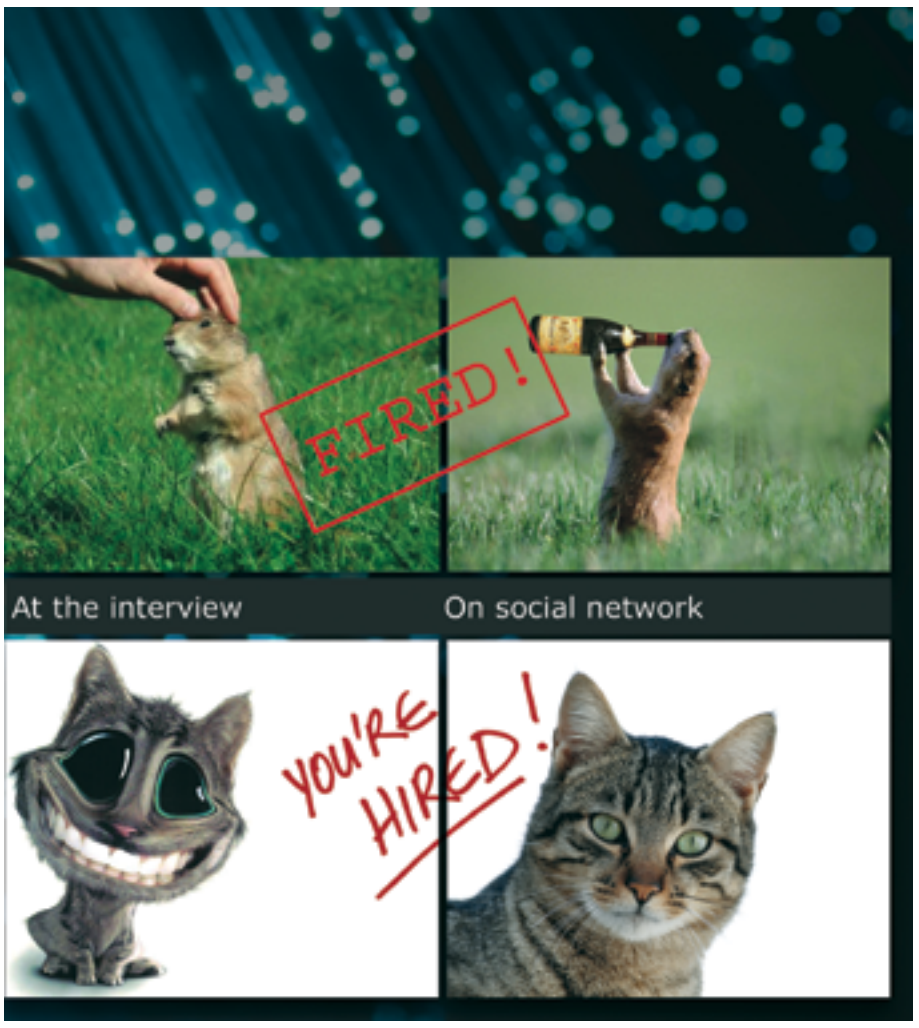
È l'interrealtà

Un termine con cui i tecnici – psicologi, sociologi - identificano quello spazio sociale in cui realtà digitale e realtà materiale si fondono mediante lo scambio continuo di informazioni sino a confondersi. L'interrealtà, la mia generazione, quella che ha vissuto l'adolescenza negli anni '80-90 per intenderci, non l'ha mai conosciuta. Vivevamo la nostra giornata utilizzando strumenti diversi per ogni nostro interesse: il libro per leggere, il telefono grigio di bachelite per telefonare, il pc 486 per giocare a fifa '92, la bicicletta per andare in piazza e incontrare gli amici, la biblioteca per le ricerche. Oggi, i bisogni dei nostri figli non sono cambiati, cercano sempre di incontrare gli amici, di giocare, di trovare risposte alle loro domande. Solo, oggi, sono cambiati gli strumenti: si gioca, si comunica, si socializza, si legge, si guardano i filmati, si ascolta la musica, ci si informa tutto su un unico strumento: lo smartphone (o il tablet) e, più in generale, la rete, il web.

Questo di per sé non è un male, anzi. Le opportunità offerte dalla rete sono infinite e ancora in gran parte da esplorare. No, il problema che stiamo solo ora cominciando ad affrontare è che i nostri ragazzi vivono in una realtà sempre più liquida, dove si mescolano disordinatamente i comportamenti tipici dell'ambiente reale, materiale, con quelli caratteristici di quello digitale. E non sempre i comportamenti adottati sono coerenti con la tipologia di ambiente vissuta. Così, ad esempio, lo scherzo banale di pasticciare il diario del compagno di scuola nell'interrealtà diventa lo scherno feroce sulla bacheca dei social: il comportamento è simile a quello delle generazioni precedenti, lo strumento no. Gli impatti no. Le conseguenze nemmeno. Prima lo scherzo era condiviso con 10, 20 persone al massimo; oggi se non si ottengono 1000 like "non si è nessuno". Prima la pagina del diario si strappava e si cestinava, oggi sulla rete non si può cancellare nulla. E dopo anni periodicamente, regolarmente, come la pinna dello squalo del famoso film, ricompaiono immagini che ancora ai protagonisti fanno male.

Di tutto questo e di tutti gli altri rischi del web, i nostri ragazzi non hanno consapevolezza. Per loro la rete è solo lo schermo nero su cui digitano costantemente: in metropolitana, a tavola, in bagno, sul divano mentre guardano la tele, a scuola mettendo le mani nell'astuccio per nascondersi dai professori. E' questa assenza di consapevolezza che non ci lascia tranquilli. Incontrando i ragazzi si percepisce il loro bisogno, a volte inespresso, a volte urlato con atti e gesti estremi, di essere aiutati. È che non sanno a chi chiederlo, questo aiuto.

D'altra parte sembra che noi genitori e insegnanti abbiamo paura che questo aiuto vengano a chiederlo. Solo il 13,6% degli adulti si sente in grado di essere un buon punto di riferimento per i propri figli sulle tematiche della rete. Viceversa, i ragazzi attribuiscono alla capacità dei loro genitori di aiutarli in rete un discreto 24,2%, che non sarà eccelso, ma comunque raddoppia quasi il livello parentale di autostima.



I dati in questo caso confermano il fenomeno di eccesso di domanda di aiuto da parte dei ragazzi rispetto all'offerta proposta dai loro genitori. Anche da qui la tendenza degli adolescenti di rivolgersi in rete ai loro pari creando un effetto whirpool senza uscita: ho un problema con la rete, mi rivolgo alla rete per risolverlo, il problema non si risolve ma s'ingrossa.

Ecco che allora la ragazza adolescente posta su siti come Ask.fm le proprie difficoltà personali, provando anche a dire che non ce la fa più e che pensa di farla finita, chiedendo ai suoi coetanei di darle un consiglio. E questo consiglio in effetti può arrivare, anzi ne possono arrivare a centinaia, a migliaia, ma non si tratta di consigli sul professionista o su chi potersi appoggiare per uscire dal tunnel.

Alla ragazza possono arrivare profonde considerazioni sulla maggiore efficacia di successo del lancio dal settimo piano piuttosto che dallo spararsi un colpo in bocca. E poi arriva, può arrivare, il consiglio dell'esperto che se proprio si vuole sparare allora deve usare questo tipo di arma piuttosto che l'altra... "Ma cosa dici? – commenta un terzo – non è importate l'arma, quello che conta sono i proiettili che usi.." e via con 5, 10 , 100, 1.000, 10.000, 100.000 like. E la ragazza comincia a pensare che se i commenti hanno centinaia di like.. bè, forse hanno ragione loro. Quando i like diventano migliaia, la ragazza pensa che sicuramente hanno ragione loro e che la scelta migliore è quella di farsi del male.

È veramente un circolo pericoloso, soprattutto per il taglio netto di comunicazione tra le generazioni: i dati raccolti sul campo dai volontari della nostra associazione ci raccontano che solo il 4,22% dei ragazzi racconta agli adulti le situazioni spiacevoli vissute in rete. Quattro per cento. Questo forse è il dato più preoccupante. Più ancora del 30% dei ragazzi che dichiara di essere stato vittima almeno una volta di casi assimilabili al cyberbullismo. Vuol dire che nel sistema manca qualcosa.

Perché noi adulti non ci facciamo trovare? Spesso diamo la colpa alla tecnologia: troppo complessa, non ne sappiamo molto e poi i nostri figli sono molto più avanti di noi. In realtà, rifugiandoci dietro questa scusa, non cogliamo le similitudini che ci sono tra l'interrealtà e la patente di guida.
Quando compie i 18 anni, il ragazzo prende la patente completando un ciclo di apprendimento che non dura solo i due mesi della scuola guida e l'esame finale, ma che è iniziato almeno quindici, sedici anni prima quando i genitori hanno cominciato a dirgli "fermati in fondo al marciapiede", "attraversa solo sulle strisce", "se è rosso, fermati", e così via. A guidare in strada o in autostrada, il ragazzo ci arriva accompagnato dagli adulti. Anche la rete – a modo suo - è un'autostrada, e i nostri ragazzi, che noi lo si voglia o meno, la percorreranno nei prossimi anni in lungo e in largo.
Lo smartphone, il tablet, la smartTV, sono le automobili con cui i nostri figli sfrecciano a mille all'ora sul WEB, ma non c'è nessuna scuola guida che dica loro come "si guidano bene" questi strumenti. Come la maggior parte delle autostrade, anche internet ci può portare in posti nuovi e bellissimi, prima irraggiungibili. Come tutte le strade ad alta velocità, però, anche il web richiede che si faccia attenzione ai pericoli e ai rischi.
Là si chiamano alta velocità, nebbia, ghiaccio, imprudenze, colpi di sonno. Qui si chiamano cyberbullismo, adescamento on line, cybercrime, gestione dell'identità digitale, dipendenza patologica del web, gioco d'azzardo on line e digital divide sociale.

E come nell'autostrada reale anche nell'autostrada digitale tutti noi, adulti e ragazzi, facciamo errori a causa delle nostre debolezze, o perché siamo convinti che gli incidenti possano capitare solo agli altri o perché ci convinciamo che "per una volta non succede mica nulla" o perché pensiamo di essere più bravi degli altri o anche solo perché vogliamo far veder al mondo quanto siamo da ammirare.
Ci sentiamo ancora peggio quando pensiamo che per il web non è necessario aspettare di essere maggiorenne. Oggi i dati ci dicono che già a 9, 10 anni si fa uso costante della rete e l'anno prossimo l'età si abbasserà ulteriormente.
Strano come pur non essendo meccanici o istruttori di guida ci sentiamo in grado di insegnare ai nostri figli a guidare bene mentre non ci sentiamo capaci di prepararli ad un uso maturo delle nuove tecnologie perché non siamo esperti di informatica.
In realtà, le competenze tecnologiche sono importanti, ma non sufficienti: per insegnare a "vivere responsabilmente" le nuove tecnologie, le competenze tecnologiche sono sì importanti ma non sufficienti.
I volontari di Icaro riescono ad essere un riferimento per i ragazzi proprio per questa eterogeneità di esperienze che portano in aula: informatica, psicoterapia, pedagogia, diritto, comunicazione. La conoscenza dello strumento è una base di partenza che, mettendosi in gioco, può essere acquisita in breve tempo grazie all'aiuto di persone competenti o anche chiedendo ai nostri figli di insegnarci. Ma da sola resta comunque unicamente una base di partenza perché qui stiamo parlando anche di comportamenti, di educazione, di buoni e sani principi.
A volte spiace deludere i genitori che vengono a sentirci nelle nostre conferenze spettacolo, ma non ci sono grandi scuse, né capri espiatori per fuggire le loro, le nostre, responsabilità.
Due sono quindi le aree su cui le statistiche e le esperienze con cui siamo confrontati in questi quattro anni di attività dell'Associazione ci hanno spinto ad investire: la prima è quella di continuare a incontrare direttamente e apertamente i ragazzi, la seconda è quella di contribuire a concretizzare una nuova tipologia di professionista della persona, attualmente non disponibile sullo scenario formativo dei ragazzi, ma da questi richiesto.
Lo specialista di Icaro incarna le caratteristiche di questo professionista: punto di riferimento per i ragazzi e gli adolescenti, ma anche per le scuole, soprattutto laddove si sono adottati pc e tablet come strumenti didattici senza grossi investimenti sulle competenze dei professori; capace di saper adottare modalità comunicative e linguaggio idonei, non solo alla didattica ma anche alla comunicazione con adolescenti e preadolescenti.
Che conosce i rischi nell'uso delle nuove tecnologie e le relative contromisure, così da essere un esperto con cui confrontarsi e non il giudice sullo scranno.
Che conosce anche le dinamiche comportamentali che caratterizzano il cyberbullismo, il sexting, l'adescamento on line , la technology addiction e il gioco d'azzardo on line così da saper riconoscere i segnali di sofferenza o rischio e da poter insegnare a sfruttare al massimo tutte le opportunità offerte dalla rete, promuovendo un uso consapevole e positivo delle nuove tecnologie finalizzato alla cooperazione, collaborazione e socializzazione.
Tre, infine, sono gli elementi fondamentali per ottenere risultati desiderati con efficacia e in breve tempo: il primo è incontrare i ragazzi nei loro abituali punti di incontro: la scuola, gli oratori, i centri di aggregazione sociale, i centri sociali, e la famiglia ovvero là dove i ragazzi sono soliti crearsi e discutere le opinioni, facendole crescere mediante il confronto tra i pari.
Il secondo, incontrarli in gruppi ristretti, quali quello tipico delle singole classi scolastiche. In questo caso, soprattutto se in assenza del giudizio di insegnanti e genitori e guidati con attenzione e sicurezza, i ragazzi sfruttano la disponibilità dell'esperto per approfondire i loro dubbi o affinare le loro domande. A volte anche per imparare e adottare comportamenti banali ma fondamentali. Il terzo, infine, è sfruttare al massimo tutte le tipologie di lavoro organizzabili con i ragazzi in funzione della disponibilità del programma di lavoro scolastico: incontri di sensibilizzazione, workshop, laboratori multimediali, laboratori emotivi sono tutti strumenti che sollecitano i ragazzi a porsi delle domande, a far nascere i loro "perché?"
Questo in fondo è l'obiettivo che la nostra ONLUS si pone: la tecnologia cambia velocemente e quello che è valido oggi, domani potrebbe non esserlo già più, ma il senso critico che sviluppiamo oggi domani sarà ancora con noi e ci permetterà di avere consapevolezza dei nostri comportamenti.
Per questo incontriamo i ragazzi e li rendiamo consapevoli dei rischi e delle opportunità che affrontano quotidianamente sul web.
E incontriamo pure i genitori e cerchiamo, anche attraverso appositi percorsi formativi, di aiutarli a comprendere meglio cosa facciano i loro figli con le nuove tecnologie e come possano evitare che si creino barriere nella loro comunicazione.
E funziona.

L'Associazione "Icaro ce l'ha fatta ONLUS", nasce nel 2011 dall'idea e dall'impegno di un gruppo di professionisti nel campo della sicurezza informatica, della psicologia, della pedagogia, del diritto e della comunicazione multimediale, convinti che la consapevolezza delle possibilità, dei limiti e dei rischi connessi all'utilizzo delle tecnologie in Rete aiuti i ragazzi a crescere e interagire con la società nel rispetto dei diritti umani e civili e della dignità della loro e dell'altrui persona. I volontari e gli specialisti dell'Associazione intervengono nei luoghi di aggregazione e formazione degli adolescenti e preadolescenti per supportare la prevenzione di forme di violenza mediatica quali, ad esempio, l'adescamento on-line, il cyberbullismo e il cybercrime, derivanti da un utilizzo improprio e pericoloso delle tecnologie diffuse.
Negli scorsi tre anni l'Associazione ha operato in 30 istituti, tra scuole Primarie e Secondarie, Centri di Aggregazione Giovanile e Oratori, in 19 città diverse, organizzando oltre 200 eventi in cui si sono incontrate più di 4000 persone di cui oltre 2800 ragazzi e più di 1200 adulti, educatori e genitori.
Altre informazioni sull'Associazione sono disponibili sul sito istituzionale www.associazioneicaro.org.

Ambienti Digitali, Democrazia e Identità Digitale: Sfide e Opportunità in Sanità. La Tempesta Perfetta

Giuliano Pozza, CIO Fondazione Don Gnocchi Milano

La Sanità digitale è, probabilmente, una delle più grandi sfide e nel contempo opportunità, che il prossimo futuro ci riserva. La progressiva digitalizzazione della società e dei servizi è iniziata con la diffusione dell'infrastruttura abilitante di Internet negli anni '90. E' proseguita con i servizi sempre più pervasivi e potenti del World Wide Web ed è ora in piena esplosione con i social media e l'Internet delle cose (o Internet of Things – IoT).

Tale crescita esponenziale della tecnologia sta creando tuttavia anche una serie di rischi, che non possono essere trascurati, se vogliamo cogliere le tremende opportunità insite nei servizi che la tecnologia ci offre. Nell'ambito sanitario queste contraddizioni emergono in modo dirompente. Infatti, guardata, ad esempio, con gli occhi di un esperto di sicurezza informatica, la Sanità dal punto di vista tecnologico potrebbe essere descritta come la "Tempesta Perfetta".

Sistemi tecnologici obsoleti, innovazione sempre più spinta su diversi fronti (social media e servizi "mobili", sistemi integrati regionali, nuove tecnologie biomedicali sempre più potenti…), culture diverse e disomogenee spesso con scarsa consapevolezza dei rudimenti di governo della tecnologia, tecnologie salvavita, che, se non gestite correttamente, possono essere un potenziale vettore di attacco letale.

Sembra un mondo progettato apposta per dare ad eventuali malintenzionati tutti gli strumenti per ottenere il massimo danno con il minimo sforzo. E in questo caso il massimo danno non è "semplicemente" economico, ma potrebbe addirittura arrivare a mettere a rischio la vita dei pazienti.

Anche senza arrivare ad ipotesi apocalittiche, il furto dei dati sanitari è già una realtà. Ci sono diverse banche dati (in particolare: www.informationisbeautiful.net), che catalogano i furti di dati per area: la Sanità, prima del 2007 quasi assente da questi report, ora è uno dei settori "meglio" rappresentati. Il rischio è in effetti elevato: un sistema in equilibrio precario, che potrebbe collassare se non verranno prese le necessarie misure e i necessari investimenti per metterlo in sicurezza. Insomma, come direbbe John Snow ("The Game of Thrones"): "When they break, they break hard!"

L'opportunità perfetta

Eppure la "Tempesta perfetta" è solo una parte della storia, una visione parziale. In realtà, la Sanità è un esempio estremamente chiaro, forse il più chiaro di tutti, di come la tecnologia possa cambiare in meglio la vita dell'uomo. Gli esempi potrebbero essere innumerevoli, ma basta scorrere gli elementi delle "Tempesta Perfetta" per capire come ciascuno di questi rappresenti anche un'opportunità. Le tecnologie salvavita, dai pacemaker alle pompe ad infusione ai defibrillatori impiantabili, sono sì potenziali vulnerabilità (anche perché costruiti in alcuni casi senza tenere in debita considerazione le regole base per garantire un livello di sicurezza adeguato), ma sono anche, come dice il loro stesso nome, strumenti che hanno salvato e salveranno la vita di un numero sempre crescente di persone. Nello stesso modo i dispositivi medicali, le diagnostiche sempre più evolute, la robotica in sala operatoria hanno contribuito drasticamente a migliorare la capacità diagnostica e terapeutica almeno nei paesi sviluppati.

L'innovazione di sistema, di cui i Sistemi Sanitari Regionali e il Fascicolo Sanitario Elettronico sono un esempio, rappresentano un potenziale incredibile per costruire e rendere possibile il difficile equilibrio tra una medicina sempre più efficace e di qualità e nel contempo dai costi sostenibili.

I social media e tutto il mondo delle App dedicate al benessere e alla salute sono (finalmente) un esempio concreto e reale di empowerment del paziente, obiettivo sempre citato in quasi ogni convegno e presentazione sul futuro della medicina, ma diventato mitico e irraggiungibile come fosse un Sacro Graal della medicina moderna.

D'altro canto, le culture diverse e spesso poco "consapevoli" dal punto di vista del buon uso e buon governo della tecnologia, insieme a infrastruttura informatiche in molti casi non adeguate, sono una sfida, ma anche una grande opportunità di miglioramento. Un terreno fertile da cui ripartire.

Ovviamente la tecnologia in Sanità va ben al di là della "tecnologia informatica", ma questa giocherà un ruolo sempre più importante anche per la convergenza tra il mondo dell'informazione e il mondo fisico, che nuove frontiere tecnologiche (nanotecnologie, robotica, stampa 3D per citarne alcune) stanno rendendo possibile.

Quasi sempre nei film di fantascienza le tecnologie avveniristiche rendono disponibili cure mediche ad oggi impensabili, espressione di un desiderio profondo di ogni uomo: quello di poter vivere una vita libera dalle malattie. Anche nel recente "Transcendence" di Wally Pfister, un film con molti limiti ma che ha il pregio di rappresentare le previsioni di scienziati e futurologi famosi come Ray Kurzweil, Hugo de Garis e Jason Silva, quando la super intelligenza artificiale vuole "conquistare" la fiducia degli uomini, applica le sue potenzialità alla medicina unendo informatica e nanotecnologie e cominciando a guarire gli abitanti del paese vicino.

Le opportunità possono essere guardate anche attraverso i trend, che stanno emergendo e che, almeno in alcune nazioni tra cui l'Italia, sono già criticità evidenti capaci di mettere in discussione il nostro stesso modello di vita: invecchiamento della società, cronicità e rischio di insostenibilità dei sistemi sanitari e di welfare. A queste sfide, la Sanità digitale può dare (e in alcuni casi già sta dando) risposte importanti. Le risposte che stanno emergendo richiederanno quasi sempre un supporto di tecnologie informatiche abilitanti. Si citano a titolo di esempio:

- la ricerca di nuove modalità di assistenza per anziani al di fuori dei contesti tradizionali (ospedali, Residenze per anziani, etc...). Questo si sposta molto bene con l'esigenza, sempre più diffusa ed espressa da parte degli anziani stessi, di essere assistiti e curati ovunque, possibile nel proprio ambiente domestico. Il tema ovviamente va affrontato a tutto tondo, come ben spiegato nel Quaderno dell'Osservatorio della Fondazione Cariplo "Abitare Leggero" (a cura di F. Giunco).

In Italia, in particolare, ci siamo polarizzati su servizi residenziali per anziani o su assistenza a casa garantita fondamentalmente da un esercito di badanti e familiari, mentre in altri paesi la gradazione dei servizi disponibili è un arcobaleno di possibilità: dalle Assisted Living Facilities alle Continuing Care Retirement Communities con tutte le possibilità intermedie presenti ad esempio negli Stati Uniti.

In molti paesi del §Nord Europa l'anziano rimane a casa propria e gli vengono offerti servizi sociali che vanno dalla spesa ai pasti portati a casa all'assistenza infermieristica. In tutti questi setting, in particolare in quelli più spostati verso il territorio, le tecnologie di teleassistenza e di telemonitoraggio rappresentano un'opportunità incredibile per conciliare l'esigenza dell'anziano di poter rimanere nel proprio ambiente, con la necessità di garantire un accompagnamento sicuro a persone che presentano spesso fragilità importanti;

- la ricerca di nuovi modelli sanitari che permettano un più efficiente utilizzo delle strutture sanitarie ad alta intensità. Nel suo libro, "The Innovator's Prescription: A Disruptive Solution to the Health Care", C. Christensen spiega molto bene come la sfida vera per rendere sostenibili i sistemi sanitari del futuro sarà quella di riuscire a gestire diversamente le malattie croniche, che nei Sistemi Sanitari dei paesi occidentali ormai assorbono oltre il 70% delle risorse per il 30% dei pazienti.

La gestione di questi pazienti dovrà sempre più spostarsi verso sistemi di assistenza territoriale. Anche qui la disponibilità di tecnologie di comunicazione, monitoraggio e cura a distanza, insieme a modelli di servizio e di remunerazione adeguati, saranno la chiave di volta dei prossimi anni.

Istruzioni per l'uso della Sanità digitale: come poter cogliere le opportunità e contenere i rischi

Tra le sfide e le possibilità offerte dalla tecnologia di cui abbiamo parlato, vi è uno spazio di azione importante, una "finestra di opportunità", che va colta ora. Siamo, infatti, in un momento storico unico. L'evoluzione tecnologia ha ormai svelato pienamente la natura "esponenziale" del suo percorso di sviluppo, come predetto da molti studiosi dalla fine del secolo scorso in poi.
A questo trend inarrestabile dobbiamo accompagnare un percorso di crescita della capacità dell'uomo di governare la tecnologia. Questo ritengo sia il punto chiave, la svolta che deciderà se andremo verso un futuro utopico o distopico.
Fino ad ora, la nostra capacità di gestire la tecnologia si è evoluta molto meno velocemente della tecnologia stessa. Credo che questo fatto sia sotto gli occhi di tutti.
Il tema è talmente evidente ormai che anche a livello europeo sono state lanciate una serie di iniziative specifiche sul tema della e-Leadership (http://www.eskills-guide.eu/home) con l'obiettivo di coinvolgere sia i professionisti dell'ICT sia tutti coloro (e sono sempre di più), che hanno o avranno un ruolo in progetti o servizi digitali, pur non essendo specialisti dell'ICT. Urgono, quindi, misure immediate, alcune delle quali sono già in atto ma vanno potenziate e velocizzate:
- costruire percorsi di formazione, sia universitari che post-universitari, perché vi sia un terreno comune di comunicazione tra figure diverse (tecnici, gestori, esperti di processo o di organizzazione, professionisti sanitari) con un minimo comun denominatore di "buoni principi" per il governo della tecnologia. Il Governo della tecnologia (o Governance of Enteprise IT, come viene chiamata da alcune organizzazioni internazionali quali ISACA), non è un tema dei tecnici o dei Direttori dei Sistemi Informativi, ma una priorità del management di ogni azienda (anche e forse soprattutto sanitaria). Un efficace governo della tecnologia è condizione "sine qua non" per ottenere valore dagli investimenti, che altrimenti rischiano nella migliore delle ipotesi di essere soldi sprecati (e nella peggiore di aumentare l'entropia del sistema).
Le maggiori università si stanno già muovendo in questa direzione: ormai il Governo dei Sistemi Informativi è oggetto di studio nei corsi tecnici, ma anche nei corsi di Economia e di Management. Il percorso va velocizzato, includendo anche facoltà tradizionalmente più caratteristiche del mondo sanitario (medicina, scienze infermieristiche etc...) e cercando di recuperare con Master o azioni formative ad hoc i professionisti sanitari, che vengono da un percorso "tradizionale", quindi molto distante da questi temi.
In quest'ottica si inserisce l'azione di AISIS (Associazione Italiana Sistemi Informativi in Sanità) e di AICA (Associazione Italiana Calcolo Automatico) denominata eHealthAcademy.
Si tratta di un percorso rivolto inizialmente ai Direttori dei Sistemi Informativi, attuali e futuri, per potenziare le loro capacità di Governo, di Leadership e di Comunicazione. Il percorso porterà ad una "qualificazione delle competenze" secondo il framework internazionale eCF e, successivamente, alla certificazione delle competenze stesse come previsto dalla norma UNI 11506. L'eHealthAcademy dovrebbe poi svilupparsi con percorso formativi ad hoc per professionisti e manager sanitari, in collaborazione con organizzazioni di categoria ed università.
- Definizione di percorsi di crescita equilibrata delle componenti di servizio ICT. Uno degli errori più comuni, che in qualche modo è legato ad una carenza di governo o di visione architetturale, è quello di investire in modo "sbilanciato" solo su alcune componenti dell'architettura. L'errore più comune è forse quello di investire più sulle nuove applicazioni, senza considerare che una infrastruttura tecnologica sicura ed abilitante è un pre-requisito.

In altri casi, si corre il rischio opposto, quello di investire enormemente in grandi "autostrade informatiche", su cui poi non circolano informazioni, perché mancano le applicazioni. I modelli architetturali più noti (citiamo solo l'Enterprise Architecture Model del NIST) o i modelli di maturità e di valutazione ormai disponibili, evidenziano bene questo tema.
Tra questi ultimi ne citiamo due: il modello di valutazione di AISIS delle aziende sanitarie e il modello "eHealth Journey" del Politecnico di Milano. Dai dati di entrambi emerge come i leader, ossia coloro che possono dimostrare un percorso di successo, hanno gestito negli anni un corretto bilanciamento degli investimenti su diversi ambiti, dalle applicazioni alla tecnologia di base alla sicurezza. Questo vale sia a livello della singola struttura sanitaria che a livello "di sistema", dove evidentemente la difformità dei sistemi informativi regionali non aiuta il percorso.
- dal punto di vista culturale e organizzativo, sarà sempre più necessario superare la tradizionale divisione tra figure professionali che lavorano spesso in modalità non integrata. La tradizionale divisione tra "utenti" o "key users", che definiscono il bisogno e i requisiti, Direzioni del Personale o funzioni qualità, che intervengono sull'organizzazione e sui processi, manager che finanziano e professionisti ICT, che progettano e realizzano le soluzioni tecniche, non è più applicabile nel contesto attuale. Sempre più sarà necessario che tutte le fasi vedano un coinvolgimento di team multidisciplinari che integrino le competenze tecnologiche, organizzative e di processo che governino il percorso insieme al management.
Per finire, credo sia importante ricordare che iniziative di sensibilizzazione di tutti i portatori di interesse, dai politici ai clinici alle associazioni di categoria ai pazienti, saranno sempre più importanti per creare il consenso necessario. Il viaggio verso una Sanità digitale non è infatti un progetto tecnologico, ma un gigantesco processo di gestione del cambiamento con impatti organizzativi, di processo e culturali enormi che richiede, per avere il successo, il coinvolgimento attivo di tutti gli attori!

Delete.
I profili, cancellati, di Akhenaton e di Nefertiti, sua sposa, inondati dai raggi solari.
(Tebe - XIV sec a.c.)

L'impatto delle soluzioni digitali per la qualità totale

Carmelo Battaglia, Direttore commerciale Pubblica Amministrazione e Relazioni istituzionali di InfoCert

La Sanità paperless rappresenta, oggi, uno dei punti fondamentali su cui l'agenda digitale punta. Per il Governo del nostro paese rappresenta una sfida importante nella consapevolezza che si tratta oramai di un processo imprescindibile.
I benefici in questo settore, dove sono entrati a pieno titolo i processi digitali, sono evidenti a tal punto che ogni investimento fatto ha avuto un ritorno in termini economici ed in termini di "qualità totale".
Relativamente al termine qualità possiamo fare un focus su tre elementi in particolare:
- certezza e sicurezza dei dati sanitari;
- nuove soluzioni nelle relazioni medico/paziente;
- dematerializzazione dei processi documentali.

In generale, possiamo affermare come le soluzioni digitali hanno avuto impatto sia dal punto di vista "sociale" che dal punto di vista "economico".
Possiamo tradurre gli effetti di cui sopra con una affermazione: produzione di salute.
Volendo esplicitare alcuni effetti che appartengono al settore della medicina, possiamo affermare che mediante tali soluzioni nel mondo "e-Health" sono entrate a pieno titolo come processi a valore i seguenti:
- remotizzazione dei rapporti medico paziente;
- sensibile eliminazione del rischio di infezioni;
- certezza di diagnosi e di terapie curative.

Ma questi processi digitali non avrebbero potuto avere le certezze di cui sopra se le applicazioni utilizzate (validate da norme di grado primario e non) non si fossero avvalse di strumenti entrati oramai in maniera usuale nei sistemi digitali, in particolare il riferimento è:
- Firma digitale e o Identity System;
- Posta Eletronica Certificata;
- Conservazione Sostitutiva a norma.

Possiamo brevemente citare come gli strumenti e le applicazioni abbiano consentito oggi di ottenere una scrivania elettronica, utile al paziente, al medico ed alla struttura sanitaria, un tipico esempio è costituito dalla "paperless help-desk ", il paziente si identifica e rappresenta le proprie esigenze ricevendo risposte in tempo reale con tracciatura di richiesta e risposta, nelle fasi successive (visite, ricoveri, referti, immagini, ecc.) egli potrà consultare o fare consultare i propri dati previa autenticazione propria (ovvero del soggetto legittimato).
Questi sistemi hanno prodotto efficienze in termini di costi valutabili nei casi in cui si è voluto quantificare il dato pari al 60%.
Certamente questi processi hanno dato un ottimo contributo alla riduzione del digital divide che, tradotto in termini di efficienza si traduce comunque e sempre in "valore".
Una forte spinta, anche nel mondo della sanità potrà venire dal Sistema di Autenticazione univoco "SPID".
Alcuni player di mercato, annoverabili tra le Certification Authority stanno portando avanti questo progetto, voluto dal Governo e "in lavorazione" sotto la super visione di AgID.
Un lavoro fondamentale e propedeutico per la costituzione del Fascicolo Sanitario Elettronico (FSE).
I documenti vengono prodotti, spediti e conservati secondo le regole che consentono agli stessi di avere valore legale e valore di conformità agli originali, pertanto vanno ad alimentare un repository personale (del soggetto fisico) formando così il Fascicolo Sanitario Elettronico.

Sicuramente le regole tecniche o le specifiche univoche, a cui tutti player di mercato e le strutture sanitarie devono adattare i loro modelli di processo consentono l'ottenimento di un sistema univoco e pertanto interoperabile sia in fase di produzione che di consultazione.
Il ruolo di coordinatore e "redattore delle specifiche" non può che essere esercitato dal Governo, il rischio di lasciare ad ognuno spazi di interpretazione e decisione porterebbe a soluzioni diverse più o meno eccellenti, ma perimetrate ed utilizzabili facilmente esclusivamente nel territorio di riferimento.

Vlad III (1431-1476). L'impatto nell'immaginario collettivo.
Vlad l'Impalatore e gli emissari turchi, che trattano la sconfitta. Theodor Aman (1831-1891)

Il Totem. La forza enigmatica del potere.
Gudea, Principe di Lagash.
Mesopotamia meridionale (2164-2144 circa a.C.),
Il primo sovrano a dichiararsi tale per volontà divina.

e-Sanit@, Rivista del Management dell'e-Healthcare
www.esanitanews.it

Direttore Responsabile: Mario Dell'Angelo
Per richiedere il Quaderno dell'Osservatorio e-Health e-Sanit@,
scrivere a: comunicazione@esanitanews.it

e-Sanit@ è un'edizione SudSanità s.a.s.
Via Alberto Mario 44 – 95127 Catania
cell 3487815738 – info@sudsanita.it

ANCOM
Autoritatea Națională pentru Administrare și Reglementare în Comunicații

ROMÂNIA
Ministerul Afacerilor Externe

SOCIAL MEDIA

VICTIMS HEROES

From Hieroglyphs to Facebook

Old and new History for the youth and those who are writing today's histories