Editoriale

Internet Festival - Forme di Futuro

Origini, motivazioni e obiettivi

Negli anni Cinquanta l'informatica era una disciplina per pochi iniziati, gli elaboratori elettronici apparivano oggetti misteriosi e gli operatori personaggi che parlavano un linguaggio esoterico e vestivano camici bianchi.

Oggi, e da tempo, le imprese del software sono al centro dell'attenzione economica, sociale e politica: il software si *è mangiato il mondo*.[1] La rivoluzione digitale ha cambiato e cambierà, con una velocità che non finisce di sorprendere, il modo in cui gli esseri umani si muovono nel mondo. I servizi e le infrastrutture delle nostre comunità vengono trasformati dall'accelerazione imposta dall'adozione di tecnologie software. L'intelligenza umana e l'intelligenza artificiale creano opportunità per modificare e potenziare l'insieme delle attività umane. Parafrasando Calvino[2], la *leggerezza del software* ha avuto la capacità di tratteggiare e condensare la complessità dei sistemi digitali in un concetto semplice: ha reso vivo un mondo immateriale, impalpabile, incorporeo ma estremamente reale.

L'avventura pisana dell'informatica prende le mosse negli anni Cinquanta dalla visione di un gruppo di scienziati, politici e industriali che, nell'affrontare le sfide della contemporaneità, immaginano un futuro dove l'innovazione tecnologica, la formazione e la ricerca in informatica siano appunto le chiavi per il cambiamento sociale, economico e culturale dell'Italia. Il progetto e la realizzazione del primo calcolatore elettronico italiano (CEP – Calcolatrice Elettronica Pisana), l'attività del laboratorio di ricerca dell'Olivetti, la creazione dell'istituto CNUCE del CNR e l'avvio nel 1969 del primo corso di laurea in Informatica - allora chiamata Scienze dell'Informazione - sono alcuni dei risultati di quella visione del futuro che fanno di Pisa la culla dell'informatica italiana. Nel 1986, il 30 aprile, è il CNUCE che realizza il primo collegamento dell'Italia alla rete Arpanet.

Il sistema dell'alta formazione e ricerca di Pisa - Università, Scuola Normale Superiore, Scuola Superiore Sant'Anna, CNR Area della Ricerca - ha

accompagnato la rivoluzione digitale contribuendo a creare le basi scientifiche e culturali su cui l'innovazione tecnologica è maturata. All'inizio degli anni Novanta l'avvento di Internet e dei sistemi e applicazioni basati sul web hanno trovato a Pisa il terreno fertile per nuove e ambiziose sfide di ricerca. Il sistema pisano è diventato sempre più aperto all'interazione con la società civile diventando lo strumento effettivo di co-creazione e diffusione dei risultati della ricerca scientifica e tecnologica in un'ottica di collaborazione responsabile tra i molteplici interlocutori del territorio.

È in questo ecosistema che proprio a Pisa nel 2011 nasce Internet Festival-Forme di Futuro (IF), evento annuale progettato per offrire un luogo aperto di dibattito interdisciplinare che aiuti a comprendere il valore e le ricadute sociali ed economiche della ricerca scientifica in Information & Communication Technologies. La ragione costitutiva di IF è la spinta a incentivare l'interazione continua tra reale e digitale, evidenziando anche il ruolo dell'affidabilità e della sicurezza nella fruizione di contenuti digitali.

Internet Festival-Forme di Futuro è una iniziativa unica nel panorama nazionale e mira a trasferire a un pubblico vasto (imprese, professionisti, cittadini e studenti) le conoscenze tecnico-scientifiche allo stato dell'arte, grazie alla forte componente accademica tra i partner. Ogni anno, in ottobre e anche successivamente, viene ideata e organizzata una pluralità di eventi sia per un pubblico non specialistico sia per esperti, con spazi appositamente dedicati alle attività di formazione delle nuove generazioni. Lo sguardo orientato al futuro, l'attenzione al presente e alle sue sfide e la volontà di comunicare le basi scientifiche dell'innovazione tecnologica con una mentalità critica costituiscono la vera ricchezza di Internet Festival, che ha raccontato il presente dell'innovazione tecnologica ma soprattutto ha cercato di delineare l'avvenire, individuando gli elementi di riflessione utili ad immaginarne le forme.

Internet Festival-Forme di Futuro è promosso da istituzioni pubbliche (Regione Toscana, Comune e Area Metropolitana di Pisa), da centri di formazione superiore e ricerca (l'Università di Pisa, la Scuola Normale Superiore, la Scuola Superiore Sant'Anna e il CNR con il Registro.it) e dal tessuto di imprese rappresentato dalla Camera di Commercio di Pisa, oltre all'Associazione Festival della Scienza.

Cosa aspettarsi da Internet Festival

IF dura quattro giorni e, tranne la prima edizione che si è tenuta nel maggio 2011, si svolge dal giovedì alla domenica della seconda settimana di ottobre. Il programma è composto da diverse tipologie di eventi.

Conferenze e seminari. In più sedi si sviluppa il dibattito sui più recenti progressi della ricerca e della tecnologia digitale e delle relative questioni etiche, sociali ed economiche. Le conferenze sono strutturate intorno a una serie di relatori principali e sessioni interattive con i partecipanti. Si propongono di

comunicare e divulgare le innovazioni scientifiche e tecnologiche in campo sia accademico, sia industriale, del settore pubblico come di quello privato.

Spettacoli. Eventi cinematografici, esibizioni teatrali e musicali, installazioni artistiche per accompagnare l'innovazione con effetti creativi non convenzionali.

Tradizione e innovazione. Incontri con i protagonisti della cultura, dello sport, dell'imprenditoria in campi un tempo lontanissimi dall'informatica. Ad esempio, appuntamenti per seguire l'evoluzione del settore agrifood nella distribuzione, comunicazione, produzione e nella fruizione del consumatore.

Mostre. Eventi interattivi e installazioni multimediali volti a presentare l'innovazione tecnologica con una prospettiva creativa e artistica.

Tutorial-Tour (T-Tour). I T-Tour sono i percorsi educativi di IF che si propongono di fornire gli strumenti per orientarsi nel mondo dell'innovazione digitale. Sono aperti ai giovani e ai nativi digitali, ai professionisti di domani, agli esperti e ai cultori della materia: nessuno deve sentirsi escluso per ragioni di formazione, età, genere. I T-Tour prevedono non solo l'abituale dimensione fisica di interazione con i partecipanti, ma anche una dimensione digitale specificatamente progettata per arricchire il progetto formativo con nuove modalità coinvolgenti e partecipative.

La popolazione studentesca pisana, toscana e nazionale è il cuore pulsante dei T-Tour. Ogni anno gli studenti, dalle primarie e alle superiori di secondo grado, li popolano per avvicinarsi ai principali temi delle tecnologie digitali. Parallelamente al programma in presenza, il Festival sviluppa anche un palinsesto online del T-Tour al fine di raggiungere gli utenti a distanza.

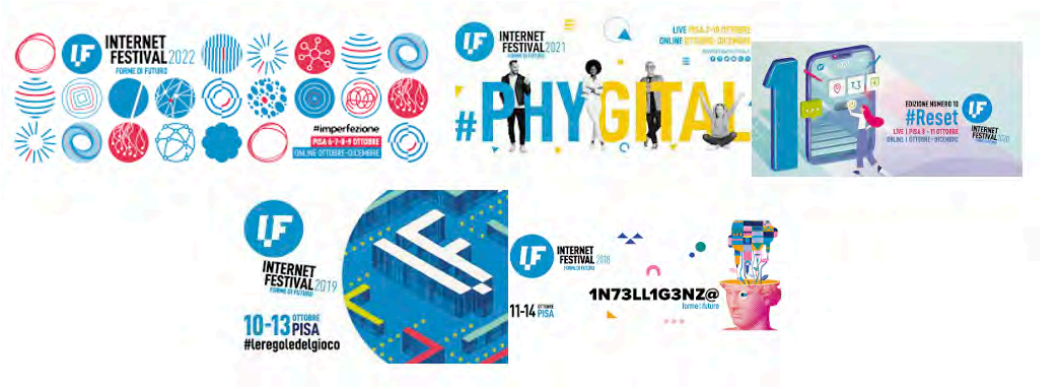
Gli eventi di IF sono gratuiti e seguiti da un pubblico eterogeneo che con curiosità ed entusiasmo vuole cogliere il senso della trasformazione digitale della società. L'insieme degli eventi permette al pubblico di toccare, osservare e riflettere sul mondo immateriale delle tecnologie digitali, all'interno di un contesto aperto, da prospettive differenti e libero da un approccio puramente accademico.

IF è un'occasione per scoprire le meraviglie del prossimo futuro digitale, ma nel contempo visitare Pisa oltre la Torre pendente.

Pillole di Internet Festival

Ogni edizione di Internet Festival è caratterizzata da una parola chiave che permette di orientarsi, osservare e interpretare tutti gli eventi del palinsesto. Le parole chiave delle ultime cinque edizioni e le relative immagine grafiche sono:

…	2018	2019	2020	2021	2022	…
	Intelligenza	Le regole del gioco	Reset	Phygital	Imperfezione	



Maggiori informazioni su Internet Festival e l'archivio di tutte le edizioni sono disponibili on line all'indirizzo https://www.internetfestival.it/.

Alcuni numeri di Internet Festival

Il 2022 è l'anno della dodicesima edizione di Internet Festival-Forme di Futuro. Presentiamo alcuni numeri complessivi. Nel 2021 i visitatori e le visitatrici, sia in presenza che a distanza, sono stati complessivamente 146.228. Nella stessa edizione sono stati registrati in particolare:

PARTECIPANTI IF 2021	MODALITÀ
22.550	In Presenza
123.678	In Live Streaming
9.756	Live Posts

La tabella seguente illustra i numeri degli eventi e dei T-Tour negli anni:

	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
Eventi	167	158	150	129	108	91	135	124	85	41
T-Tour	35	62	82	63	59	52	62	64	47	63

I T-Tour sono il cuore pulsante di IF non solo i termini di partecipazione, ma anche in base alle valutazioni ottenute, con tecniche di Data Analytics, dal sondaggio distribuito agli insegnanti che hanno partecipato all'Internet Festival 2021. La stragrande maggioranza (81%) ha utilizzato il materiale e le conoscenze acquisite nei T-Tour nelle successive lezioni. Solo una piccola percentuale (13%) ha risposto di non aver utilizzato in classe quanto presentato durante i T-Tour. Inoltre, il 100% dei partecipanti al sondaggio ha dichiarato di aver acquisito competenze significative dagli eventi a cui hanno partecipato.

La misurazione dell'impatto sociale di Internet Festival è sempre stato uno degli aspetti significativi dell'iniziativa. Il progetto Me-Mind[3], finanziato dalla EU, ha come obiettivo la misurazione l'impatto socio-economico di eventi culturali sul territorio in cui operano. Il progetto vede come partner del consorzio la Fondazione Sistema Toscana e il Dipartimento di Informatica dell'Università di Pisa, e IF è uno dei suoi due casi studio. Durante l'edizione del 2021, Me-Mind ha promosso la realizzazione di un'installazione artistica interattiva, *Il nodo della cultura*, grazie alla quale è stato distribuito al pubblico un questionario composto da più di 30 domande. L'installazione ha raccolto 521 questionari in italiano e 25 questionari in inglese. Di seguito riportiamo alcuni risultati dell'analisi condotta sul data set dei questionari compilati in italiano.

Un primo risultato ha riguardato le preferenze del pubblico in base alla tipologia di eventi e fasce di età. I partecipanti di età inferiore ai 15 anni sono risultati più interessati alle tematiche dell'innovazione digitale e della transizione ecologica. Quelli di età compresa tra i 16 e i 25 anni, invece, tendono a rivolgere maggiore interesse alle ricadute sociali e culturali dell'innovazione digitale. I partecipanti di età compresa tra i 26 e i 35 anni sono i più interessati a comprendere l'impatto dell'innovazione digitale sull'ambiente e le trasformazioni culturali. I partecipanti di età compresa tra i 36 e i 45 anni esprimono una elevata preferenza verso le tematiche culturali mentre. Quelli di età compresa tra i 46 e i 55 anni mostrano interessi equamente divisi tra le tematiche culturali e quelli ambientali. Gli interessi dei partecipanti di età compresa tra i 56 e i 65 anni sono equamente distribuiti tra tutte le tematiche del festival con una leggerissima preferenza per l'innovazione tecnologica. Infine, i partecipanti di età superiore ai 65 anni mostrano due tendenze contrastanti. Il primo gruppo non sembra particolarmente interessato a nessuna tematica in particolare. L'altro gruppo mostra un buon interesse per tutte le tematiche con una leggera preferenza per quelle sociali e culturali.

Il questionario somministrato prevedeva domande intese a misurare il livello di gradimento dei partecipanti a Internet Festival-Forme di Futuro in una scala di valori che andava da 1 (valore minimo) a 10 (valore massimo). Il livello di gradimento è stato calcolato tenendo conto del genere, delle professioni legate al settore dell'istruzione (insegnanti e studenti). Complessivamente, il grado di soddisfazione medio è elevato: la media del livello di gradimento degli insegnanti è di 8,64, quella degli studenti è 7,93. Relativamente al genere, le

donne mostrano un grado di soddisfazione più elevato rispetto agli uomini (7,89 contro 7,78). Da notare che il gruppo di visitatori identificato come "genere diverso" ha espresso il più alto grado di soddisfazione (8,85).

Conclusioni

Internet Festival negli anni è diventato l'appuntamento nazionale che fa il punto sui temi della transizione digitale, accogliendo visitatori da ogni parte d'Italia ed esperti nazionali e internazionali. Inoltre, è uno strumento che valorizza adeguatamente la mole della conoscenza del sistema dell'alta formazione e della ricerca pisano e lo rende fruibile al grande pubblico. Infine, permette di comunicare l'eccellenza del sistema Italia in modo efficace facendo crescere il livello di attrattività complessiva del nostro paese. Non è da trascurare l'effetto sull'immagine e sull'economia della città per la quale la manifestazione è diventata un asset la cui importanza strategica, culturale e turistica è stata riconosciuta dalle amministrazioni comunali che si sono succedute negli anni.

Adriana De Cesare,

Fondazione Sistema Toscana, Internet Festival Project Leader

Gian-Luigi Ferrari

Dipartimento di Informatica, Università di Pisa

Coordinatore Comitato Scientifico Internet Festival

Claudio Giua

Direttore Internet Festival

Anna Vaccarelli

Iistituto di Informatica e Telematica (IIT) - CNR Pisa,
Coordinatore Comitato Esecutivo Internet Festival

[1] *Marc Andressen "Why Software Is Eating The World" (The Wall Street Journal Agosto 2011*
[2] *Italo Calvino, "Lezioni americane. Sei proposte per il prossimo millennio, 1. Leggerezza", 1985*
[3] *https://www.memind.eu*

Laudatio in occasione della Laurea honoris causa in Computer Science al Dott. Gastone Garziera, Università degli Studi di Bari Aldo Moro, 14 ottobre 2019

Stefano Ferilli

Alla stragrande maggioranza delle persone, il termine “computer” richiamerebbe alla mente il familiare oggetto, compagno quotidiano di mille attività, posizionato sulla scrivania, se non proprio nella borsa da lavoro o addirittura in tasca. Difficilmente si penserebbe ad un mostro tecnologico che possa occupare un’intera stanza o un edificio, gestito da personale in camice bianco a cui chi fosse interessato a svolgere dei calcoli automatici deve rivolgersi, come a dei sacerdoti in un tempio, per chiedere il responso dell’oracolo e sperare di ottenerlo, salvo intoppi, dopo qualche giorno. Eppure è questo che accadeva fino a pochi decenni orsono, negli anni sessanta. Non solo l’idea stessa di computer era ancora legata a quella di “centro di calcolo” alla portata di pochissime e facoltose organizzazioni; molti ne ignoravano persino l’esistenza. A quell’epoca sarebbe stato difficile, se non impossibile, per chiunque, e specialmente per gli addetti ai lavori, immaginare che quello strumento avrebbe mai potuto starci su un tavolo, a disposizione di una sola persona. Il “Personal Computer” sarebbe nato solo un decennio più tardi, grazie ad un’incredibile serie di eventi e coincidenze che si materializzarono nella Silicon Valley (all’epoca la Bay Area di San Francisco, perché il silicio non ne era ancora diventata la principale fonte di ricchezza) attorno ad un gruppo di persone i cui nomi oggi sono quasi leggendari (citando Federico Faggin, Chuck Peddle, Steve Jobs, Steve Wozniak si fa certo torto a tanti altri meno noti ma non meno importanti).

In un tale contesto, ben dieci anni prima dell'invenzione del microprocessore, che ha dato il via all'Informatica come la conosciamo oggi, solo degli illuminati (qualcuno avrebbe detto "pazzi") visionari avrebbero potuto concepire, e provare a realizzare, il sogno di un computer "personale", delle dimensioni di una calcolatrice. Ebbene, questi "pazzi visionari" ci furono, e furono in tre. Fra il 1962 ed il 1964, sotto la guida dell'Ing. Prof. Pier Giorgio Perotto, e sotto la protezione di Natale Capellaro (anche lui laureato *honoris causa* di questa nostra Università, in una continuità che oggi ci fa piacere sottolineare), questa squadra di visionari riuscì, in gran segreto, a progettare e costruire, presso la Olivetti, il primo concetto di "personal computer" della storia: la *Programma 101*. Una pietra miliare dell'Informatica e un orgoglio italiano che fu presentato nel 1965 alla grande esposizione di prodotti per ufficio BEMA di New York, dove molti visitatori furono convinti che le sue sorprendenti prestazioni fossero dovute a un grande calcolatore nascosto dietro le quinte. Seppur con la tecnologia dell'epoca, essa esprimeva esattamente il concetto odierno di Personal Computer, anche se tale termine non sarebbe stato coniato se non oltre un decennio dopo. Stava comodamente su una scrivania ed aveva la possibilità di essere programmata, di ricevere input tramite tastiera e di emettere output tramite stampante, ed era dotata perfino di un dispositivo di memorizzazione di massa portatile nella forma di schede magnetiche, l'equivalente dei futuri dischetti. Ebbe un successo enorme, soprattutto negli Stati Uniti, dove concorse alle elaborazioni necessarie allo sbarco sulla luna.

Di quel ristrettissimo gruppo di lavoro faceva parte Gastone Garziera, all'epoca neodiplomato, che contribuì così a scrivere una pagina storica, e a realizzare una pietra miliare, per l'Informatica mondiale. Egli ha partecipato attivamente all'intero sviluppo della *Programma 101*: progettazione dell'Unità logico-elettronica, collaudo dei vari livelli prototipali, completamento dell'integrazione di prodotto. Danno testimonianza di tutto questo un'ampia letteratura e persino un film documentario. Quest'esperienza unica è stata solo l'inizio di una carriera densa di contributi significativi e di innovazioni drastiche allo stato dell'arte dell'informatica, che hanno anche indirizzato l'evoluzione tecnologica nella direzione di cui oggi cogliamo i frutti.

Nel corso della sua carriera, Gastone Garziera ha continuato a partecipare, con ruoli sempre più rilevanti, alle attività informatiche della Olivetti, da cui sono scaturite macchine d'avanguardia per l'epoca e di estremo interesse storico oggi, anche alla luce di come le tecnologie informatiche si sono poi sviluppate. Gli incarichi ricoperti, sia con ruoli operativi che di direzione, hanno spaziato dall'hardware al software, dallo sviluppo alla ricerca.

Contribuisce alla impostazione dei prodotti derivati dalla P101: P102, P203, Logos328, e la famiglia della Logos270. Dal 1968 al 1973 è responsabile di progetto (a capo di un gruppo di 7/8 progettisti) della **P 652**, orientata al mercato tecnico-scientifico. Dal 1973 al 1976 è responsabile *come Product manager e di progetto HW e FW*, del **Sistema P6060-P6066** (Personal Computer classico *ante litteram*). Dal 1976 al 1978 è *responsabile dello sviluppo dei sistemi di fascia media* per i settori scientifico, word processing e gestionale. Dal 1979 al 1985 partecipa alla ricerca e definizione *della prima piattaforma*

Hardware della Olivetti, ed è *responsabile della ricostruzione ed evoluzione dei sistemi Software dei prodotti specializzati precedenti* (a capo di un gruppo di c.ca 80 progettisti interni e 30 esterni). Dal 1985 al 1987 è *responsabile della costituzione e gestione* nel comprensorio di Ivrea *dei gruppi di Progetto PC, dei Monitors, delle Tastiere, e degli Alimentatori*. Dal 1987 al 1990 è *responsabile della Ricerca e Sviluppo della Divisione Retail*, che sviluppa Hardware specifico, Software di base ed applicativi per la gestione delle vendite con un gruppo di c.ca 100 progettisti interni e 30 esterni. Dal 1990 al 1992 è *responsabile della Direzione Qualità per la Ricerca e Sviluppo* (un gruppo di c.ca 120 persone). Da fine '92 è *responsabile della Direzione Qualità per la Divisione Prodotti* (che comprende lo sviluppo e la produzione degli Office Products, Stampanti e Personal Computer). Dal 1993 al 1995 è *responsabile dei laboratori di Pozzuoli di Olivetti Ricerca* (per un totale di oltre 200 ricercatori). Da metà '95 fino alla pensione cura i piani di formazione per i Progettisti Olivetti.

Le attività di sviluppo a cui ha partecipato hanno portato a significativi avanzamenti o addirittura rivoluzioni dello stato dell'arte ed anche al riconoscimento di numerosi brevetti di cui 8 a suo specifico nome. Sarà il caso di ricordarne qui solo alcune pietre miliari.

Nella Programma 101 furono notevoli la scelta della Linea Magnetostrittiva come memoria, superando i problemi di variazione del tempo di percorrenza; l'introduzione dei "micromoduli" e della metallizzazione dei fori nella realizzazione dei circuiti stampati; il linguaggio di programmazione, simbolico, di sole 15 istruzioni semplici ed intuitive, adatto anche ad utenti non specializzati; l'introduzione dei salti a "label" invece che indirizzanti, il che rendeva il codice "autorilocante"; e l'invenzione del primo supporto magnetico discreto, la Cartolina Magnetica, copiato dalla HP, che riconobbe alla Olivetti 900000 $ di royalties nel 1969.

Lo sviluppo della P652, iniziato nel 1968, introdusse la tecnica originale del FW quando **i microprocessori non esistevano ancora**. Il linguaggio utente, realizzato attraverso la **microprogrammazione** in ROM, era semplice, richiedeva tipicamente un ciclo macchina per l'esecuzione, e gestiva **subroutines con 5 livelli di nesting ed interrupt**. Il **RISC, presentato ben 17 anni dopo, nel 1985, aveva esattamente i principi fondamentali della UC della P652**. Singolare, per quei tempi, l'**algoritmo usato nel calcolo dei logaritmi**, basato sulla proprietà matematica che il logaritmo di un prodotto è uguale alla somma dei logaritmi dei fattori.

Il P6060, la cui progettazione iniziò nel 1973, aveva già Sistema Operativo su Floppy disc o su Hard disc, Linguaggio BASIC con funzioni grafiche, Tastiera alfanumerica+funzioni, uscita su stampante-plotter e video grafico, e varie interfacce standard per la comunicazione esterna. Sebbene fosse previsto il FW in ROM, **Garziera propose e ottenne di tenerlo in RAM**, dotando invece la ROM di funzioni di diagnostica iniziale, di acquisizione delle risorse disponibili, e di caricamento e lancio del FW e SW del caso. **Questo assetto** di fatto **definì il *modus operandi* di tutti i PC da lì in poi, operante ancora oggi**. La scelta innovativa di dotare la macchina di due canali di interfaccia seriale è **poi**

diventata una dotazione Standard dei PC, presente ancora oggi come USB. Il monitor grafico gestito a bitmap fu **praticamente l'invenzione dei pixel**.

Nello sviluppo dei sistemi Retail **Garziera promosse la realizzazione di un ambiente di controllo qualità** che, sostituendo le tastiere con un robot, era **in grado di collaudare in modo automatico tutte le fasi di vita del sistema,** e lavorava in continuazione, giorno e notte, liberando gli operatori umani per progettare nuovi test invece che eseguirli.

Dopo il pensionamento, avvenuto nel 1996, Gastone Garziera ha instancabilmente lavorato per la diffusione della cultura informatica, per la costruzione di una coscienza storica dell'industria informatica italiana e della sua rilevanza mondiale, per la diffusione della cultura informatica in generale specialmente presso i giovani. Numerose e preziose sono state le attività divulgative aventi ad oggetto le innovazioni tecnologiche che ha contribuito a sviluppare nell'arco della sua carriera. Sono sicuramente da ricordare quelle in ambito istituzionale (nel 2015 riceve il **Simbolo della Presidenza del Consiglio dei Ministri**), universitario, Scolastico e Didattico, aziendale, museale e storico-collezionistico. Dal 2006 intraprende l'attività di **volontariato al LaboratorioMuseoTecnologic@mente** di Ivrea, Museo-Laboratorio didattico incentrato sulla storia industriale della Olivetti, contribuendo al recupero funzionale di varie macchine d'epoca.

L'attività di Gastone Garziera ha dunque coperto tutte le direzioni in cui un'università moderna deve muoversi: ricerca e innovazione, didattica e terza missione. La sua opera ha portato lustro all'Italia nel mondo. Chi meglio di lui può essere da esempio per tutti coloro che in questi obiettivi si riconoscono e che di questa Università fanno parte? Per questo siamo felici di poterlo annoverare da oggi fra i nostri laureati, e di potergli dire di cuore: grazie, Dottor Garziera!

Innovazioni tecnologiche alle origini dell'informatica "personale"

Gastone Garziera

1. La Valle dell'EDEN

Ritengo doveroso iniziare descrivendo l'ambiente dove si è concretizzato lo studio che ha portato alla Programma 101: Il LABORATORIO RICERCHE ELETTRONICHE OLIVETTI

IL LRE è nato quando Adriano Olivetti ha accettato l'invito dell'Università di Pisa a partecipare allo sviluppo della CEP (Calcolatrice Elettronica Pisana).

Adriano partecipò con finanziamenti, apparecchiature, ed un gruppo di Persone. Questo gruppo di progettisti si costituì attorno a Mario Tchou, che Adriano aveva individuato mentre, completati gli studi in USA, stava insegnando alla Columbia University. Lo convinse a rientrare in Italia ed a mettersi a capo di quello che sarebbe diventato appunto il LREO. Era il 1955.

Questo gruppo, una volta impostata la CEP, si separò dall'Università per perseguire gli obiettivi Olivetti, che erano divergenti da quelli dell'Università. Si spostò prima a Barbaricina, vicino a Pisa, poi a Borgolombardo, a sud di Milano, in attesa di spostarsi nella sede definitiva, che Adriano aveva voluto a Pregnana Milanese, a nord di Milano. Dove alla fine il LRE si spostò a cominciare dalla fine del '62.

Questo gruppo costituito inizialmente da un manipolo di persone, si incrementò strada facendo arrivando, agli inizi degli anni '60, a superare le 200 unità.

Quello che sorprende sono i risultati raggiunti, in tempi che mi sembrano particolarmente brevi.

Dopo il lavoro svolto per la CEP, basato sulla tecnologia delle valvole termoioniche, il LRE cominciò a pensare a computer di tipo commerciale.

Realizzò un primo prototipo tutto a valvole, che fu impiegato per la gestione di un magazzino Olivetti, l'ELEA 9001.

Passò poi ad un secondo prototipo, l'ELEA 9002, con parti già a transistor (se non erro le unità nastro). Questo prototipo fu usato per la gestione della Consociata Italia.

A questo punto, Mario Tchou decise di puntare ad un prodotto tutto a transistor. E nel 1959 la Olivetti lanciò l'ELEA 9003, primo calcolatore al mondo completamente a transistor.

Credo che Adriano, forse non solo lui, avesse capito da tempo che la tecnologia della lamiera di ferro, tranciata e piegata, aveva dato, con le macchine meravigliose di Natale Capellaro, tutto quello che poteva dare, ed aveva consentito alla Olivetti di diventare grande. Ma, per garantire la crescita della Olivetti, che per Adriano era lo strumento fondamentale per il raggiungimento dei suoi obiettivi (il benessere della "Comunità"), era necessario trovare una nuova tecnologia. Si era convinto che questa tecnologia fosse l'elettronica. Vedi il laboratorio con il fratello Dino, a New Canaan, Connecticut, per lavorare sulle tecnologie dei computer. Vedi anche i suggerimenti di Enrico Fermi. E colse al volo l'occasione fornita dall'Università di Pisa.

E cominciò a creare la simbiosi fra i prodotti Olivetti, soprattutto le fatturatrici-contabili, ed i calcolatori, in particolare l'ELEA 9003, che si sarebbe installata a partire dal 1960.

Nacquero così il CBS (convertitore banda schede, progettato da Perotto), ed il CBN (convertitore banda nastro), che convertivano la banda prodotta dalle Audit nelle schede ed i nastri, che l'ELEA sapeva leggere.

E nacque l'UME (unità moltiplicatrice elettronica), che, aggiunta alle Audit, ne accresceva enormemente la produttività.

Sviluppati contemporaneamente alle ELEA.

Il LRE era costituito da chi integrando le parti generava il computer, ma anche da una serie di laboratori che presidiavano e facevano evolvere le varie tecnologie.

Alcuni esempi: Unità magnetiche (nastri), Memorie (a nuclei), Circuiti (prima al germanio, poi al silicio), Laboratorio di Fisica, ecc.

Chi aveva necessità per il suo progetto, poteva attingere e chiedere sviluppi specifici.

La Valle dell'EDEN.

2. La Linea Magnetostrittiva

Al primo incontro, quando l'ing. Perotto ci parlò della richiesta del dott. Roberto Olivetti, ragionando insieme, alla fine fu chiaro che dovevamo puntare ad una macchina che stesse su una scrivania, che fosse facile da usare, che costasse il meno possibile, e che, visto che fatta di elettronica sarebbe costata sicuramente più delle macchine meccaniche, doveva avere funzionalità che ripagassero il maggior costo. Queste furono di fatto le specifiche funzionali che pilotarono il nostro lavoro.

Ci disse anche che voleva provassimo a realizzare un marchingegno che facesse qualche operazione, ma che usasse una memoria del passato, una linea magnetostrittiva. Aveva già chiesto al laboratorio di Fisica di farne un prototipo. La memoria a nuclei era ritenuta troppo complessa e costosa per il nostro obiettivo, mentre la linea di ritardo magnetostrittiva era la memoria costruttivamente più semplice che si potesse immaginare: un filo con una testina di scrittura (noi ne avevamo due alla distanza di un carattere) da un lato, una testina di lettura dall'altro lato, con un amplificatore.

Così, attorno al rudimentale prototipo di LMS fornito dal laboratorio di Fisica, fu realizzato un cosiddetto "feasibility model", con il quale era possibile fare semplici operazioni, tipo somme fra numeri relativi e, se non ricordo male, la moltiplicazione di un numero per un digit. Si stampava su una telescrivente araba.

L'esercizio del "feasibility model" ci lasciò la convinzione che riuscivamo a dominare quella strana memoria dinamica, con i bit che continuavano a correre, che la scelta dell'architettura, penso canonica, era quella giusta, ed anche la rappresentazione numerica in decimale con virgola naturale andava bene, ed in definitiva meritava proseguire con quel tipo di memoria.

La distribuzione dei bit in memoria, detta a registri interallacciati, si realizza affiancando i bit omonimi di tutti i registri in pacchetti, 8 pacchetti di bit consecutivi realizzano un byte di tutti i registri, e tutta la memoria è costituita da 24 pacchetti di 10 byte, 240 byte (1920 bit).

Ogni pacchetto di bit una volta letto si tiene in parallelo in un registro HW, e rimane disponibile alla logica per le operazioni sui registri e fra registri, per tutto il tempo di lettura del pacchetto successivo. Il risultato in uscita dalla rete logica si scrive poi in sequenza in linea. È ovvio che è semplice trasferire un registro in un altro, o scambiare due registri fra di loro, o sommare due registri, ad ogni giro di linea.

In questa organizzazione, particolarmente semplice è risultata l'unità aritmetica, costituita da una rete di 6 o 7 gate ed un flip-flop (per il riporto). La rete ha 3 ingressi: Operando A, Operando B e Riporto dal bit precedente, e due uscite : la Somma (binaria) ed il riporto attuale (da usare come preset del relativo flip-flop).

La realizzazione del feasibility model ci fece anche scoprire un comportamento della LMS che costituì un serio problema, che risolvemmo solo più tardi. La gestione era stata realizzata in modo sincrono, la temporizzazione era generata da un quarzo, e la linea era lunga un numero preciso di microsecondi (bit). La posizione delle testine era regolabile in modo da poter realizzare le condizioni volute.

Quando il tutto si mise a funzionare, si scoprì che il sistema era stabile per un po' di tempo, poi si perdeva il sincronismo e tutto si confondeva.

L'analisi del problema ci fece capire che la velocità degli impulsi meccanici sulla linea era funzione della temperatura, tanto ambiente, quanto quella dovuta all'energia delle correnti nelle testine.

La scoperta ci aveva non poco preoccupato. Avevamo pensato a cose strane, come lamine bimetalliche ed altri ammennicoli.

Alla fine, la soluzione fu di implementare una gestione asincrona. La linea era un po' più lunga dello stretto necessario. La temporizzazione rimaneva attiva per tutto il tempo richiesto dal numero di bit (1920), poi si bloccava, e ripartiva quando usciva il primo bit, che si fece in modo che ci fosse sempre.

Questa soluzione di fatto risolse non solo la deriva termica, ma consentì di sostituire il quarzo con un oscillatore bloccabile, di non curare troppo la lunghezza del filo nella costruzione delle linee, ed assorbì tutte le varianze dovute alle tolleranze di tensioni e componenti, ed eliminò la necessità di tarature.

In fin dei conti, un bel risultato.

3. La Programmabilità ed il Linguaggio

Nelle discussioni sul modo di dare un valore alla macchina per giustificare il maggior costo dell'elettronica, ci convincemmo che una macchina in grado di eseguire calcoli di una certa complessità, come quelli ripetitivi, che richiedevano a molte persone di dedicare lunghi periodi a fare calcoli, con calcolatrici meccaniche, avrebbe avuto un appeal di tipo commerciale. L'ing. Perotto aveva dovuto fare, durante un impiego passato (alla FIAT Avio?), lunghi periodi di calcoli ripetitivi, per definire superfici aeronautiche. Ci disse che aveva provato soddisfazione nel definire le "formule" per i calcoli, ma un grandissimo disagio nell'eseguire per lunghi periodi, i calcoli, appunto con una macchina da calcolo meccanica.

Dopo alcuni tentativi di definire una macchina a "learn", ci convincemmo che la soluzione più convincente era quella di una macchina programmabile. Come target ci eravamo posti la soluzione dell'equazione di 2° grado.

La macchina che definimmo fu una macchina di 10 registri di 24 byte ciascuno, 1920 bit in tutto.

Fu un compromesso fra dimensione di memoria per dati e programmi, e tempo di esecuzione delle operazioni. Dato il tipo di memoria, il tempo di esecuzione delle operazioni era un multiplo di giri di linea, quindi più era lunga (capace) la linea, più era lenta l'esecuzione.

I 10 registri sono: M, A, R, B, C, D ,E, F, "P2", "P1".

M, A, R, sono i registri operativi.

In particolare M contiene il 2° operando, o l'unico, e vi si formano i numeri introdotti da tastiera.

A contiene il primo operando, ed alla fine delle operazioni riceve il risultato.

R è il registro di appoggio durante le operazioni, alla fine della divisione contiene il resto.

P1 e P2 sono dedicati a contenere solo istruzioni di programma, non sono indirizzabili e non sono visibili dall'utente. Quando la macchina è in stato di "introduzione programma", le istruzioni cominciano a formarsi in P1 e dopo le prime 24, cominciano a formarsi in P2. Se il programma supera le 48 istruzioni, comincia ad invadere i registri F, poi E e D. Ogni istruzione occupa un byte.

I programmi possono essere composti al massimo da 120 istruzioni.

I registri B e C, possono contenere solo numeri.

Le istruzioni, un byte di 8 bit, sono composte per 4 bit dal codice della istruzione stessa, e gli altri 4 bit rappresentano il campo indirizzo. Il campo indirizzo è formato da 3 bit di codice di registro, in quanto i registri indirizzabili sono 8. Il quarto bit serve ad indirizzare la seconda parte di un registro numerico. I registri numerici possono contenere numeri lunghi al massimo 22 cifre, oppure, se i numeri sono al massimo lunghi 11 cifre, ne possono contenere 2, uno per ogni metà.

I registri sono individuati dal loro tasto specifico, tranne il registro M, che avendo il codice “0”, se non si batte un tasto di registro, automaticamente rimane indirizzato M. Per indirizzare la seconda metà di un registro si aggiunge il 4° bit digitando il tasto specifico : “/”, chiamato anche “split”.

I numeri sono decimali, con virgola naturale, rappresentati da digit binari, che vengono mantenuti con coerenza decimale. Ogni digit è rappresentato da un byte, in cui 4 bit sono il codice, e 4 sono di servizio (digit significativo, virgola, segno, indice).

Il linguaggio è costituito da 15 istruzioni. È un linguaggio simbolico, ogni istruzione è individuata da un simbolo e da un tasto in tastiera. La sequenza delle operazioni per il calcolo di una espressione, viene data secondo la notazione “polacca inversa”. Non è presente il tasto “=”, in quanto non necessario.

Le istruzioni sono le seguenti.

1. “Start-stop”. (Codice 0) La memoria vuota è piena di questa istruzione. Quando incontrata nel programma, si ferma l’esecuzione, si libera la tastiera ed il controllo passa all’operatore. Digitando in questa situazione il tasto “S” relativo, l’esecuzione del programma riprende dal punto in cui si era fermato.
2. “Freccia in su” o “Trasferimento”. (Codice 2) Copia il contenuto di M nel registro indirizzato.
3. “Freccia in giù” o “Richiamo”. (Codice 1) Copia il contenuto di A nel registro indirizzato.
4. “Doppia freccia” o “Scambio”. (Codice 3) Scambia il contenuto di A e del registro indirizzato fra di loro.
5. “Più”, “Meno”, “Per”, “Diviso” (Codici 4, 5, 6, 7, rispettivamente) Eseguono le rispettive operazioni fra A ed M ed il risultato si forma in A. Se è indicato un registro nel campo indirizzo, prima dell’operazione viene copiato il registro in M.
6. “Radice quadrata”. (Codice 8) Estrae la radice quadrata di M ed il risultato viene messo in A. Se è indicato un registro nel campo indirizzo, prima dell’operazione viene copiato il registro in M. Questa istruzione fu aggiunta solo all’ultimo prototipo.
7. “Stampa”. (Codice 9) Stampa il contenuto del registro indirizzato.

8. “Stampa e azzera”. (Codice 10) Stampa il contenuto del registro indirizzato, che poi viene azzerato. Da programma esegue solo l’azzeramento.
9. (Codice 11). Non usato nella P101. Sarà usato nelle evoluzioni P102 e P203 con il significato di “Invio ad apparecchiatura esterna”.
10. “Salti V, W, Y, Z “. (Codici 12, 13, 14, 15) Con il campo “indirizzo di registro” si creano coppie di codici in cui uno è il comando di “saltare”, e l’altro è il punto da cui “riprendere” l’esecuzione del programma. I codici con il bit “/” a zero hanno il significato di salto incondizionato. Quelli con il bit “/” ad uno, hanno il significato di salto condizionato, cioè il salto verrà eseguito solo se il contenuto di A è positivo. Inizialmente l’istruzione di salto era indirizzante, cioè era una istruzione bicarattere in cui il secondo carattere dava l’indirizzo da cui riprendere la sequenza di programma. Arrivammo alla soluzione finale dopo un confronto, suggerito dall’ing. Perotto, con un programmatore esperto, Leandro Alfieri, che collaborava con i gruppi di programmatori dell’ELEA 9003. Anche se ci costò tre codici istruzione in più, lo adottammo in quanto rendeva molto più semplice la gestione dei programmi. Infatti, in caso di modifiche, la soluzione indirizzante avrebbe implicato la modifica agli indirizzi di salto. La soluzione di salto a riferimento invece non richiedeva alcun ricalcolo a fronte di modifiche al programma. Di fatto il codice della P101 si può definire auto rilocante.

4. Le Dimostrazioni del primo Prototipo ed il Riconoscimento della Necessità di uno Strumento per Registrare e Rileggere i Programmi Sviluppati

Riporto la successione di attività ed eventi che ci portarono alla realizzazione del primo prototipo.

Una serie di progettazioni di unità logiche, con ripartenze al variare della disponibilità di memoria che veniva dichiarata, che rimaneva comunque sempre insufficiente per le nostre esigenze. Ciò fino all’acquisto di unita di LMS sul mercato che consentì, attraverso una attività di reverse engineering, da parte di un gruppettino di progettisti (Bruno Visentin e Carlo Oddone Passarella) di ottenere capacità adeguate.

A riprova della validità della scelta della LMS, riprogettammo l’UME in pochissime settimane ottenendo una drastica diminuzione dell’elettronica, (da 9 a 2 piastre). Fu un risultato molto convincente.

La scoperta che un gruppo di progetto meccanico, il gruppo del sig. Franco Bretti, aveva già progettato un stampantina che si adattava perfettamente alle nostre esigenze fu un vero colpo di fortuna. Questa scoperta consentì all’ing. Perotto di far gravitare l’attività del gruppo del sig. Bretti a supporto del nostro progetto.

L'arrivo del transistor al silicio, sulla base del quale il laboratorio circuiti aveva definito una base circuitale completamente nuova: il NOR ad RTL. Praticamente il concetto di "GATE", un'unica funzione logica con la quale realizzare tutte le reti necessarie.

Completammo la definizione del linguaggio (non c'era ancora la "radice quadrata"), ci arrivò anche un prototipo di tastiera, e su questa base realizzammo un progetto completo di macchina programmabile.

Completata la costruzione su piastroni filati, cominciammo il debugging. Arrivammo alla fine del '63, inizio '64 con il prototipo su rack funzionante. Procedevamo con ottimizzazioni per diminuire per quanto possibile il numero di componenti.

L'ing. Perotto invitava spesso suoi amici, ai quali facevamo delle dimostrazioni. Invitò anche il prof. Luigi Dadda, ed il dott. Ugo Galassi, direttore commerciale della Olivetti.

Fu proprio durante quelle dimostrazioni che capimmo che la macchina così definita aveva un problema, costituito dal fatto che tutte le volte che si doveva eseguire un programma diverso, era necessario digitarlo ex novo a mano. I programmi potevano arrivare a 120 istruzioni, il che poteva implicare l'esecuzione di centinaia di digitazioni. Ciò, oltre a richiedere tempo, rendeva poi necessario, tutte le volte, rifare un debugging. Tutto quello che si fa a mano può introdurre degli errori.

Ci convincemmo che la macchina doveva essere dotata di uno strumento che consentisse di "Registrare" i programmi una volta completati, e di poterli poi "Rileggere" tutte le volte che serviva, senza doverli ridigitare. Oggi si direbbe di "fare il Save" ed il "Download" delle "App".

Ci mettemmo a cercare una soluzione convincente, che alla fine si concretizzò nella cartolina magnetica, praticamente l'invenzione del primo supporto magnetico discreto. Infatti fu brevettato, e chi lo copiò (HP) dovette pagare le royalties.

Noi ripartimmo per un altro livello di prototipo, approfittando del quale introducemmo, oltre alla cartolina, e la radice quadrata, anche molte evoluzioni ingegneristiche.

Il prototipo, che divenne pronto verso la fine del '64, fu poi carrozzato provvisoriamente dal gruppo di meccanici, con una lamiera blu, e divenne la "Perottina".

5. La Dimostrazione a Natale Capellaro

Diciamo subito che nella seconda metà del '64 la situazione era molto cambiata.

La Olivetti aveva di fatto ceduto la Divisione Elettronica, con tutto il LRE, tutto tranne il gruppo di Perotto. Noi eravamo ancora a Pregnana, ospiti, ma facevamo riferimento ad Ivrea.

In particolare facevamo parte dei gruppi di progetto di Ivrea, che avevano come riferimento Natale Capellaro.

La Olivetti, secondo il volere del “Gruppo di Intervento”, doveva dimenticarsi dell’elettronica e puntare tutto su una nuova linea di macchine meccaniche. È evidente il rischio per la nostra attività. L’ing. Perotto ci spingeva a velocizzare per quanto possibile il completamento del prototipo. Ci disse: “Non voglio andare a dire che abbiamo delle idee, voglio far vedere una macchina funzionante!”.

A noi (De Sandre ed io) venne la paura che al mondo qualcun altro stesse progettando qualcosa di simile, e magari arrivasse a presentarlo prima di noi.

Morale, avevamo tutti la voglia di concludere quel progetto, che alla fine ci convinceva, eravamo tutti convinti che era innovativo, ed avrebbe potuto avere uno spazio commerciale.

Fu un periodo di attività frenetica.

Appena completata la messa a punto della parte elettronica, con la stampantina, la tastiera e la cartolina già stabili, il prototipo fu portato al gruppo dei meccanici, ad Ivrea (San Lorenzo), dove appunto fu carrozzato provvisoriamente.

Dopo il varo interno, Perotto invitò Capellaro per presentargli la macchina ed avere il suo parere.

Ricordo molto bene quell’evento. Nella sala dimostrazione c’erano un bel po’ di persone. In mezzo c’era la Perottina. Io dovevo anche fare parte della dimostrazione ed ero vicino alla macchina. Quando Capellaro arrivò, Perotto lo accompagnò alla macchina e facemmo la dimostrazione. Tutto OK. Perotto si mise a spiegare un po’ il funzionamento, compreso quello della LMS. Alla fine concluse facendo capire che aspettava il suo parere. Che non arrivò subito. Capellaro era diventato pensieroso. Nella sala si era fatto un silenzio assoluto, non si sentiva una mosca volare. La tensione era alle stelle.

Alla fine Capellaro risollevò la testa, mise una mano sulla spalla di Perotto e disse: “Caro ingegnere, vedendo questa macchina, capisco che l’Era del calcolo meccanico è finita !”

6. Il Lancio al BEMA di NY

Nonostante lo scetticismo del management, che puntava tutto sulla nuova linea di calcolatrici meccaniche, LOGOS 27, fu deciso di presentare la P101 al Bema di New York. La presentazione fu fatta bene, con tanto di “Convention”. Al Bema fu presentata inizialmente alla chetichella. Ma, appena fu scoperta dalla stampa specializzata, che capì il valore innovativo della 101, gli organizzatori furono costretti a dedicare alla P101 lo spazio centrale dello Stand Olivetti-Underwood, ed organizzare un percorso obbligato per consentire a tutti i visitatori di avvicinarla.

Il successo fu molto grande, ci furono anche clienti importanti, come la NASA e HP.

Fu poi presentata anche in Europa, e fu prodotta in 44000 esemplari.

Il management, sempre scettico, insisteva sulla meccanica. Sosteneva che non ci si poteva aspettare di venderne molte di P101, perché il mercato non

richiedeva una macchina di quel genere. La dimostrazione lampante stava nel fatto che nessun concorrente della Olivetti avesse ancora presentato una macchina simile.

Come progetto ci mettemmo a ricavare prodotti derivati.

Una calcolatrice, togliendo programmabilità e cartolina: la Logos328

Una fatturatrice, aggiungendo una macchina per scrivere attrezzata per stampare su comando della 101: la P203.

Una macchina con interfaccia verso altre apparecchiature: La P102.

Tutte con la tecnologia RTL-NOR della P101.

Alla fine tradussi la logica della Logos328 in logica DTL, micrologici dual-in-line. Fine ’66, inizio ’67.

Visto poi che non arrivavano input per attività successive, mi consultai con De Sandre, e convenimmo che mi conveniva intanto andare a fare il servizio militare. Tanto non me lo toglieva nessuno.

Partii nella primavera (Aprile?) 1967.

7. I Successori

Quando tornai, dopo aver fatto il servizio militare, a metà Luglio del ’68, il laboratorio da Pregnana si era trasferito a Milano, in via Camperio, proprio in centro. E lì era stata portata anche la mia scrivania. E l’ing. Perotto era diventato capo della Ricerca e Sviluppo Olivetti, una delle strutture funzionali.

De Sandre mi disse subito che l’HP stava lanciando una macchina concorrente della P101, l’HP9100. Lo aveva saputo, in anteprima per amicizia, da un suo ex compagno di scuola, diventato responsabile commerciale HP in Italia.

In Olivetti non si era ancora pensato ad un prodotto successore della P101. C’erano state voci che il Management voleva che prodotti di quel genere fossero sviluppati negli Stati Uniti, alla Olivetti-Underwood praticamente. Ma non era successo niente, in Olivetti si era abituati che le macchine una volta attrezzate, rimanevano in produzione 10 o 12 anni. De Sandre dovette in fretta e furia avviare un gruppo ad Ivrea (con a capo Angelo Subrizi), per sviluppare una evoluzione della P101. Per avere risultati veloci era stata avviata una macchina basata su LMS con capacità doppia (a NRZ), linguaggio evoluzione di quello P101, programmi in ROM per funzioni trigonometriche ed esponenziali. Sarebbe diventata la P602.

Io fui incaricato di uno studio con più respiro, con architettura ispirata ai minicomputer. Inizialmente si pensava ad un “posto di lavoro”, con UC, Memoria a nuclei e Rom a trasformatori.

Fui affiancato da un perito neodiplomato e neoassunto: Sandro Graciotti. Una volta capito cosa si intendeva per UC, ci mettemmo a progettarne una orientata ai nostri obiettivi. Nacque una UC essenziale, a 12 bit di indirizzamento, che trattava digit a 4 bit con gestione anche del riporto decimale, che gestiva subroutine con nesting a più livelli, gestione degli interrupt, e con la capacità di sondare livelli in input, e di generare livelli in output. Il risultato fu una CPU

semplice, a DTL, veloce, con la quale definimmo uno “Pseudo linguaggio” in termini di chiamata a subroutine che rese efficientissimo lo sviluppo dell’interprete del linguaggio utente. Ricordo che il microprogramma della moltiplicazione in virgola mobile, alla fine era composto da poco più di 20 (23 ?) microistruzioni. Inoltre fu possibile gestire da microprogramma tutte le periferiche integrate. Tanto per fare un esempio, da UC si generavano direttamente le forme d’onda di registrazione della cartolina magnetica, su due piste contemporaneamente, con controlli per garantire la correttezza e la portabilità fra macchine, che meritarono il riconoscimento di brevetto.

Stesso discorso per la gestione della tastiera, uno dei primi esempi di tastiera elettronica, con relativo brevetto.

La macchina, P652, con l’avvento delle Ram e Rom a semiconduttori, fu riorganizzata a desk top, adottando le nuove tecnologie, ed uscì nella primavera del ’73.

Quando uscì, nel ’73, incrociò una concorrenza agguerrita. Ma il suo costo accessibile, la disponibilità molto ricca di periferiche (IPSO), e di Hard Disc a testine fisse molto veloce, le consentirono una discreta posizione. Anche in velocità risultò più veloce dell’HP9830, top di gamma HP. Mi fu riportato che HP aveva considerato la P652 una “Tough Competition”.

Con lo sviluppo sulla sua base di un linguaggio tipo GTL, fu adottata per la preparazione dei comandi per le macchine a controllo numerico della OCN. Ogni istallazione OCN prevedeva così anche le P652.

Il linguaggio proprietary, con l’avvento del Basic, rappresentò comunque un handicap.

Ci rendemmo conto, anni dopo, quando vennero presentati i RISC (intorno al 1985?), che l’Unità centrale della P652 era un Risc ante litteram.

Comunque i prodotti di tipo tecnico-scientifico non ottenevano in Olivetti risultati molto soddisfacenti. La Olivetti aveva buona penetrazione negli ambienti commerciali e bancario.

Così la direzione della DPO (direzione pianificazione operativa), mandò un suo esponente, l’ing. Mauro Caprara, product planner del settore, negli Stati Uniti a cercare un prodotto OEM, da usare dopo la P652, evitando così di progettarlo in casa, e liberando risorse.

Fui mandato anche io come esponente del progetto.

Visitammo varie aziende del settore (come Wang, Compucorp, ecc.). Stavano più o meno tutti pensando a macchine basate su cassette di nastro magnetico.

Durante il rientro, proposi uno schema di macchina orientata al BASIC, basata su Floppy disc. Visto che era più evoluta di tutto quello che avevamo sentito, ci fu consentito di avviarne il progetto. Nacque così il P6060- P6066. Approfittando della presenza sistematica del disco integrato, mettemmo in ROM solo un programma che controllava le risorse disponibili, e poi caricava il sistema operativo da disco, e lo lanciava. Quella architettura divenne di fatto quella di riferimento per tutti i PC, e, se non erro, è in uso ancora oggi. Era il 1976.

Con quel prodotto, Olivetti avviò l'attività per la gestione dei risultati di Campionati di sci, e per le gare di Formula 1.

8. Conclusioni

Dopo la morte di Adriano Olivetti (Febb. '60), e di Mario Tchou (Nov. '61), la Olivetti fu costretta a cedere (prima metà del '64) alla GE americana la Divisione Elettronica, LRE compreso, ed a perdere il Know How dei calcolatori elettronici (a parte il gruppettino di Perotto). Inoltre fu spinta a puntare di nuovo il suo futuro su una linea di macchine da calcolo meccaniche. Ma, quando fu chiaro che l'elettronica si imponeva, nonostante i ritardi, merito anche dell'esperienza della P101 e derivati, la Olivetti seppe trasformarsi in azienda elettronica ed informatica, ed oltre.

Credo un caso più unico che raro.

La sicurezza cibernetica in Italia: sfide e opportunità per le PMI alla luce dell'evoluzione normativa

Luisa Franchina, Andrea Lucariello, Alessandro Calabrese e Francesco Ressa

Sommario

Il presente contributo affronta la tematica dell'evoluzione normativa in materia di cybersecurity, ripercorrendo le più recenti innovazioni, introdotte e in discussione, nel panorama nazionale ed europeo. In questo contesto particolare rilevanza viene data alla realtà delle piccole e medie imprese (PMI) e alle sfide che queste ultime devono fronteggiare, attraverso un'analisi delle minacce cibernetiche e dei possibili nuovi scenari in cui potranno essere coinvolte. Viene inoltre approfondita la rilevanza di strumenti di riduzione della complessità, come Framework e Linee Guida, utili per governare il rischio cyber.

Abstract

This article addresses the issue of cybersecurity laws and their evolution over time, referring to the most recent innovations, introduced and still under discussion, in the Italian and European landscape. In this context, a particular importance is given to small and medium-sized enterprises (SMEs) and to the challenges they have to face, through an analysis of cyber threats and possible new scenarios in which they may be involved. The relevance of complexity reduction tools such as specific frameworks and guidelines, which are useful for managing cyber risk, is also analyzed.

Parole chiave: Cybersecurity, Laws, Threats, SMEs, Risk, Scenarios

1. Introduzione

Secondo l'ultimo aggiornamento del rapporto Clusit 2021[1] in riferimento all'anno 2020, quest'ultimo è risultato essere il "peggiore di sempre" in termini di evoluzione e di crescita delle minacce cyber e dei relativi impatti. A livello globale sono stati riscontrati 1.871 attacchi gravi, ovvero attacchi aventi un impatto sistemico sia in ambito sociopolitico sia in ambito economico e produttivo.

Dall'analisi del panorama italiano è emersa una correlazione tra l'aumento del trend degli attacchi e l'insorgenza del virus SARS-CoV2. Infatti, per affrontare la pandemia, le imprese, sia pubbliche sia private, hanno dovuto fare ampio ricorso a modalità di lavoro da remoto che hanno comportato una riorganizzazione dei processi lavorativi legati a tecnologie informatiche. Lo spostamento dell'ambiente di lavoro da una struttura organizzata e "sicura", quale la sede aziendale, all'ambiente domestico, ha aumentato esponenzialmente la superficie di attacco dei cybercriminali. Questi ultimi approfittando della situazione di emergenza hanno potuto sfruttare vulnerabilità umane, organizzative e tecnologiche generate, ad esempio, dall'assenza di precise istruzioni relative alla sicurezza del lavoro da remoto o dalla mancanza di adeguati strumenti di difesa cyber (infrastrutture ICT, firewall, VPN, ...). Come menzionato dal rapporto, infatti: "i cyber criminali hanno sfruttato la situazione di disagio collettivo, nonché di estrema difficoltà vissuta da alcuni settori - come quello della produzione dei presidi di sicurezza (ad esempio, delle mascherine) e della ricerca sanitaria - per colpire le proprie vittime".

Quanto emerso dall'analisi del Clusit trova conferma anche nel Documento di Sicurezza Nazionale, all'interno dell'apposita sezione nella Relazione annuale del Dipartimento delle Informazioni per la Sicurezza (DIS) al Parlamento[2], che ha lo scopo di descrivere lo stato della minaccia cyber in Italia identificando le principali attività intraprese per la protezione cibernetica e la sicurezza informatica. In particolare, tale documento ha evidenziato, tra il 2019 e il 2020, un incremento degli attacchi informatici rivolti in particolar modo verso le Amministrazioni locali, per quanto concerne le PA, e verso organizzazioni operanti nel settore farmaceutico/sanitario, per quanto riguarda il settore privato.

Alla luce dello scenario descritto, a livello nazionale si sta delineando un percorso di rafforzamento dell'architettura nazionale di sicurezza cibernetica, iniziato nell'ultimo decennio, tramite il recepimento di una serie di norme europee che mirano ad accrescere la resilienza cyber del Paese assicurando, contestualmente, "unicità di indirizzo e un alto livello di coordinamento attraverso un approccio univoco a una materia complessa e trasversale a diversi settori e realtà"[3].

---

[1] Clusit - Rapporto 2021 sulla Sicurezza ICT in Italia.

[2] Relazione 2020 sulla politica dell'informazione per la sicurezza.

[3] DIS - Documento di sicurezza nazionale 2020, Allegato alla Relazione annuale al Parlamento ai sensi dell'art. 38, comma 1 bis, legge 124/2007.

2. Evoluzione della cybersecurity nel contesto nazionale ed europeo

La rapida evoluzione tecnologica degli ultimi anni e il contestuale mutamento delle minacce cyber ad essa correlate ha accelerato la predisposizione di un quadro normativo volto a identificare strumenti in grado di realizzare un assetto difensivo, nazionale ed europeo, rispetto allo scenario cibernetico attuale. A tal proposito, l'Unione Europea ha intrapreso un percorso volto a raggiungere un livello adeguato di sicurezza delle reti e a definire procedure comuni per il riconoscimento e la gestione dei rischi al fine di incrementare il grado di sicurezza comune.

A tal riguardo, uno dei primi passi portati a compimento a livello nazionale è stato il recepimento, attraverso il decreto legislativo 18 maggio 2018 n. 65, della cosiddetta Direttiva NIS[4]. La norma contiene disposizioni e misure volte a conseguire un elevato livello di sicurezza delle reti e dei sistemi informativi in ambito nazionale. Le prescrizioni sono rivolte agli Operatori di Servizi Essenziali (OSE), ossia quei soggetti che forniscono un servizio essenziale per il mantenimento delle attività economiche e sociali fondamentali, la cui fornitura dipende dalle reti e dai sistemi informativi, che operano nei settori relativi a: energia, trasporti, banche, mercati finanziari, sanità, fornitura e distribuzione di acqua potabile. La Direttiva si applica anche ai Fornitori di Servizi Digitali (FSD), ossia società che forniscono servizi quali motori di ricerca, cloud computing e commercio elettronico. Il decreto attuativo esplicita che entrambi le tipologie di soggetti sono tenute ad adottare misure tecnico-organizzative "adeguate" alla gestione dei rischi e alla prevenzione degli incidenti informatici. Sia gli OSE sia gli FSD devono, inoltre, rispondere a specifici obblighi che prevedono l'inoltro delle notifiche di incidenti informatici con impatto rilevante sui servizi forniti al Computer Security Incident Response Team (CSIRT) italiano. Sono stati individuati e designati, quali Autorità competenti NIS, cinque ministeri (Sviluppo Economico, Infrastrutture e Mobilità Sostenibile, Economia e Finanze, Salute e Ambiente e Tutela del Territorio e del Mare) nonché, limitatamente a determinati ambiti, le Regioni e le Province Autonome.

Coerentemente con quanto previsto della Direttiva e dal relativo decreto di recepimento, il Presidente del Consiglio dei ministri ha adottato una strategia nazionale di sicurezza cibernetica che definisce opportune misure preventive, di risposta e di ripristino dei servizi impattati da incidenti informatici, individua un piano di valutazione dei rischi informatici e propone programmi di formazione e sensibilizzazione nonché un piano di valutazione dei rischi e di ricerca e sviluppo in materia di cybersecurity.

A compimento del percorso di evoluzione normativa in ambito cibernetico è stato emanato il D.L. n. 105 del 2019 (convertito e modificato dalla Legge 18 novembre 2019, n. 133) che ha istituito il Perimetro di sicurezza nazionale

[4] DIRETTIVA (UE) 2016/1148 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 6 luglio 2016 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.

cibernetica (PSNC). Tale Perimetro è costituito da un insieme di soggetti pubblici e privati, aventi sede nel territorio nazionale, che erogano funzioni essenziali per lo Stato. In questo senso, nell'ambito delle infrastrutture ICT necessarie per l'erogazione delle funzioni essenziali, tali soggetti devono garantire un adeguato livello di sicurezza delle reti, dei sistemi informativi e dei servizi informatici in uso. In quest'ottica sono stati identificati funzioni e i servizi essenziali, di diretta pertinenza dei soggetti, che dipendono da reti, sistemi informativi o servizi informatici la cui interruzione o compromissione comporterebbe un pregiudizio[5] per la sicurezza nazionale. In attuazione del D.L. n. 105 sopra citato, è stato emanato il DPCM 30 luglio 2020, n. 131, che fornisce i criteri per l'individuazione dei soggetti che devono essere inclusi nel PSNC.

I soggetti compresi nel Perimetro sono inseriti all'interno di un elenco annualmente aggiornato dalle Autorità referenti per i singoli settori di competenza (es. Ministero delle Infrastrutture e della Mobilità Sostenibile, Ministero dell'Economia e delle Finanze ecc.).

L'implementazione del PSNC è proseguita con il DPR n. 54 del 5 febbraio 2021, che disciplina le procedure e i termini delle valutazioni condotte dal Centro di Valutazione e Certificazione Nazionale (CVCN) e dei Centri di Valutazione del Ministero degli Interni e del Ministero della Difesa sui prodotti in fase di acquisizione da parte dei soggetti inclusi nel Perimetro.

Successivamente, il 14 aprile 2021, è stato pubblicato il DPCM n. 81 relativo alle notifiche degli incidenti e alle misure di sicurezza che i soggetti sono tenuti ad attuare. In particolare, tale decreto affrontata tre tematiche principali:

- La tassonomia degli incidenti, che identifica due livelli di gravità degli stessi;
- Le modalità e le tempistiche di notifica degli incidenti;
- L'elenco delle misure di sicurezza da attuare, basate sul Framework Nazionale per la Cybersecurity e la Data Protection[6].

Con riferimento all'ultima tematica citata, tale Framework, ispirato al Cyber Security Framework del National Institute of Standards and Technology (NIST), rappresenta uno strumento particolarmente utile per misurare la postura in termini di cybersecurity di un'organizzazione. Nello specifico, il Framework propone, in maniera strutturata e con l'utilizzo di un linguaggio comune, una serie di elementi utili ai soggetti pubblici e privati per monitorare il proprio stato di sicurezza direzionando anche percorsi di miglioramento.

---

[5] Decreto-legge 21 settembre 2019, n. 105: *"il danno o pericolo di danno all'indipendenza, all'integrità o alla sicurezza della Repubblica e delle istituzioni democratiche poste dalla Costituzione a suo fondamento, ovvero agli interessi politici, militari, economici, scientifici e industriali dell'Italia, conseguente all'interruzione o alla compromissione di una funzione essenziale dello Stato o di un servizio essenziale"*

[6] CIS-Sapienza, CINI Cybersecurity National Lab, *Framework Nazionale per la Cybersecurity e la Data Protection*, febbraio 2019

Infine, il 15 giugno 2021 è stato pubblicato il DPCM riguardante le categorie di beni, sistemi e servizi ICT destinati ad essere impiegati nel PSNC. Per le categorie individuate all'interno del DPCM, qualora un soggetto intenda procedere all'affidamento di forniture destinate ad essere impiegate sulle reti o sui sistemi informativi e/o per l'espletamento dei servizi informatici relativi ai servizi essenziali erogati, è prevista una comunicazione obbligatoria al CVCN o ai Centri di Valutazione.

L'ultimo tassello a conclusione del quadro normativo relativo al PSNC consisterà in un decreto attuativo in merito agli aspetti di regolamentazione dei laboratori accreditati di prova (LAP) per l'effettuazione di screening tecnologici.

Ulteriori elementi normativi a livello europeo attualmente in fase di discussione, resi necessari dal cambiamento dello scenario cibernetico in costante evoluzione tecnologica e dalla massiva interconnessione di strumenti e servizi, sono la cosiddetta Direttiva NIS 2 e la Direttiva CER.

La prima, presentata dalla Commissione Europea il 16 dicembre 2020, si pone tre obiettivi: elevare la consapevolezza degli stati membri e del tessuto produttivo in merito ai rischi cibernetici, potenziare il livello di risposta comunitaria a eventuali emergenze e migliorare il sistema e gli strumenti con i quali la Comunità monitora i rischi. Tra le novità della NIS2 vi è l'abbandono delle categorie Operatori di Servizi Essenziali e Fornitori di Servizi Digitali a favore di nuove denominate Entità Essenziali (settori strategici come l'energia e l'acqua, i trasporti, i mercati finanziari, la salute, l'erogazione di credito, la pubblica amministrazione) ed Entità Importanti (come poste, rifiuti, settore alimentare e servizi digitali). Tutte le grandi e medie imprese che afferiscono a tali settori saranno tenute, dunque, a rispettare le norme di sicurezza previste dalla nuova normativa.

In aggiunta, è previsto, per le organizzazioni, l'obbligo di monitorare una serie di fattori chiave, tra cui la risposta agli incidenti, la catena di fornitura e l'utilizzo della crittografia.

In parallelo, e a completamento della nuova Direttiva NIS, la Commissione Europea ha avviato un processo di elaborazione della Direttiva sulla Resilienza delle Entità Critiche (CER) intesa come evoluzione della Direttiva 114/08 sulle Infrastrutture Critiche Europee (ICE). Tale avanzamento consentirà di formare un impianto legislativo omogeneo in grado di rafforzare le difese in ambito cyber, tramite una mappatura dei rischi che coinvolgono più nazioni in diversi ambiti produttivi. La nuova Direttiva individua dieci settori di attività essenziali da proteggere: salute, trasporti, banche, energia, infrastrutture dei mercati finanziari, acqua potabile, acque reflue, infrastrutture digitali, spazio e Pubblica Amministrazione. Sono inoltre previsti numerosi interventi innovativi. In primo luogo, tutti gli stati membri devono elaborare un'analisi nazionale dei rischi al fine di individuare le Entità Critiche e successivamente adottare una strategia di resilienza. Le aziende dei settori sopra elencati hanno l'obbligo di dotarsi di un piano tecnico-organizzativo in grado di potenziare la resilienza e di comunicare tempestivamente ai responsabili nazionali minacce o eventi di cyber attacco. Le Entità Critiche che forniscono servizi ad almeno un terzo delle nazioni facenti

parte della UE, inoltre, saranno sottoposte a una particolare vigilanza da parte della Commissione. La nuova direttiva CER prevede che la Commissione offra agli stati e alle società inserite nella lista delle Entità Critiche diversi tipi di supporto, come ad esempio, programmi di formazione e simulazione di incidenti. Infine, viene istituito il Critical Entities Resilience Group, composto da professionisti di livello europeo, con l'obiettivo di agevolare l'attuazione della Direttiva e la cooperazione tra gli stati membri.

Per favorire l'applicazione dell'attuale panorama normativo italiano è stata istituita l'Agenzia per la Cybersicurezza Nazionale (D.L. 14 giugno 2021, n. 82), che di fatto rappresenta un ulteriore passo in avanti verso la costituzione di un apparato organizzativo efficiente in materia di sicurezza informatica. La nuova Agenzia ricopre il ruolo di Autorità per la Cyber security Nazionale e per il coordinamento tra i soggetti pubblici coinvolti in materia di cybersecurity a livello nazionale. Tra i suoi compiti vi è anche la promozione e la realizzazione di iniziative comuni finalizzate alla sicurezza e alla resilienza della sfera cyber del sistema-Paese.

La nuova Agenzia, che, tra le altre cose, include il Computer Security Incident Response Team (CSIRT) e il Nucleo di Sicurezza Cibernetica (NSC), si presenta come un ente autonomo rispetto alle altre agenzie di intelligence, ricoprendo un ruolo nevralgico all'interno del Paese. Tra le sue funzioni rientrano alcune di quelle precedentemente attribuite alla Presidenza del Consiglio, al Ministero dello Sviluppo Economico, al DIS e all'Agenzia per l'Italia Digitale così come le competenze in materia di Perimetro di Sicurezza Nazionale Cibernetica. L'Agenzia è quindi competente anche per l'elaborazione della Strategia nazionale di sicurezza cibernetica e per il supporto alle attività del Nucleo per la cyber sicurezza, e rappresenta anche l'Autorità nazionale competente e il punto di contatto unico in materia di sicurezza delle reti e dei sistemi informativi. Essendo anche Autorità nazionale di certificazione della cybersecurity, l'Agenzia svolgerà tutte le attività relative alle certificazioni esercitate fino ad ora dal Ministero dello Sviluppo Economico da parte dei competenti organi, quali il CVCN. In aggiunta, l'Agenzia si occuperà anche della prevenzione, del monitoraggio, del rilevamento, dell'analisi, delle risposte e della gestione di incidenti di sicurezza informatica e degli attacchi cibernetici. Infine, ma non meno importante, la nuova struttura è incaricata di incrementare il coinvolgimento delle Università e degli istituti di ricerca e del sistema produttivo nazionale, nel campo della cybersecurity e ha quindi il compito di promuovere formazione, crescita tecnico-professionale e qualificazione delle risorse umane nel campo della sicurezza informatica, anche attraverso l'assegnazione di borse di studio, di dottorato e di assegni di ricerca, favorendo l'attivazione di percorsi formativi universitari.

3. La dimensione della cyber security nelle PMI

L'insorgenza e la seguente evoluzione della pandemia Covid-19 hanno contribuito al mutamento dello scenario cibernetico già in atto negli ultimi anni. In particolare, realtà appartenenti alla categoria PMI hanno dovuto confrontarsi con aspetti, in precedenza poco considerati, quali la continuità operativa aziendale e lo smart working con le relative implicazioni in termini tecnologici e

di sicurezza. La rapidità con cui le PMI si sono dovute adattare alle nuove sfide del "lavoro da remoto" ha comportato una prioritizzazione degli aspetti operativi a discapito di quelli afferenti alla sicurezza informatica, ove non già consolidati. Tale scenario, come dimostrato dal numero crescente di incidenti di cybersecurity, ha aumentato la superfice d'attacco cibernetica, esponendo le organizzazioni ad eventuali attacchi e, conseguentemente, incentivando gli avversari a condurre azioni malevole. Tra i principali elementi da attenzionare, che possono costituire ambiti futuri su cui intervenire, vi sono la scarsa consapevolezza rispetto alle minacce cyber, i costi di attuazione delle misure di difesa e l'assenza di figure tecniche specializzate.

Questo è ciò che si evince dal report Cybersecurity e Data Protection: l'evoluzione del contesto e lo scenario di mercato in Italia dell'Osservatorio Cybersecurity & Data Protection[7], che riporta:

> *"Dal quadro generale emerge come la particolare situazione legata all'emergenza sanitaria abbia causato importanti stravolgimenti anche all'interno delle piccole e medie imprese: il 54% del campione ha dichiarato che si è trovata costretta a lavorare da remoto, e, tra queste, il 36% ha dovuto adattare le modalità di lavoro al nuovo contesto. Le realtà più piccole si sono spesso attrezzate in modo non strutturato al nuovo scenario, con impatti dal punto di vista della cybersecurity: l'utilizzo da parte dei dipendenti di device personali e reti domestiche dal basso livello di protezione ha esposto maggiormente le aziende ai rischi di sicurezza, come confermato dal 59% del campione. Il 49% delle PMI ha peraltro rilevato, nell'ultimo anno, un importante aumento degli attacchi informatici, spesso basati sul fattore emotivo e sulla ricerca di informazioni in tema pandemia."*

Nonostante le criticità rilevate, il rapporto evidenzia come la sicurezza informatica sia ancora una tematica sottovalutata dalla maggior parte delle organizzazioni. Infatti, solo il 22% delle aziende analizzate ha predisposto investimenti in tal senso per il 2021, mentre il 27% del campione dichiara di non ritenere rilevante la sicurezza informatica. Gli investimenti, in generale, sono prevalentemente indirizzati sulla componente tecnologica, con particolare riguardo nei confronti di soluzioni di sicurezza di base quali firewall e antivirus, mentre rimangono pressoché marginali le cifre destinate all'introduzione di competenze specifiche e di figure professionali quali Security Analyst o Security Administrator.

[7] https://www.yarix.com/wp-content/uploads/2021/04/Cybersecurity-e-data-protection-levoluzione-del-contesto-e-lo-scenario-....pdf

Questa tendenza trova conferma anche nel report dell'Agenzia dell'Unione europea per la cyber sicurezza (ENISA) "Cybersecurity for SMES Challenges and Recommendations" pubblicato nel giugno 2021[8].

Dall'indagine condotta da ENISA si evince come la maggior parte delle PMI (più dell'80%) tratti informazioni "critiche", ossia informazioni, spesso di natura sensibile, la cui perdita produrrebbe all'organizzazione ripercussioni legali, operative e di perdita di know-how.

Nonostante le PMI utilizzino alcune accortezze in materia di sicurezza, come antivirus, firewall e backup, queste non risultano, il più delle volte, sufficienti a garantire un'adeguata protezione contro le minacce cibernetiche. Inoltre, risulta notevolmente basso il numero di aziende che predispone corsi di sensibilizzazione in materia di cybersecurity, dinamica che evidenzia una mancanza di interesse verso attività di diffusione della consapevolezza rispetto alla dimensione cibernetica.

Non stupisce pertanto che, per quanto riguarda la tipologia di attacchi, i più diffusi siano stati il phishing, gli attacchi web-based e i malware, in particolar modo i ransomware (il mercato legato ai pagamenti di riscatto risulta in netta crescita). L'esposizione a tali tipologie di attacchi, infatti, può essere significativamente ridotta attraverso percorsi volti ad aumentare la consapevolezza e a garantire una formazione di base del personale aziendale in materia di sicurezza cibernetica.

Uno scenario con queste caratteristiche può incentivare la comparsa di forme estorsive cibernetiche, una sorta di "cyber pizzo", nelle quali gli attaccanti potrebbero mettere in atto tre comportamenti differenti. In primo luogo, considerato il livello di sicurezza delle PMI, potrebbero proporsi di proteggere le vittime dagli attacchi di altri attori malevoli dietro pagamento; in secondo luogo, potrebbero minacciare l'esecuzione di eventuali attacchi nel caso in cui le PMI non pagassero il riscatto richiesto dagli attaccanti stessi; in terzo luogo, potrebbero offrire protezione a seguito di un attacco andato a buon fine, perpetrato, in maniera anonima o meno, dagli attaccanti stessi al fine di evidenziare le vulnerabilità delle PMI.

La propensione delle vittime ad accettare o subire questa condizione potrebbe risultare elevata e concreta, soprattutto per le realtà più piccole, alla luce della mole di attacchi e dei relativi impatti di tipo economico-reputazionale.

Se da un lato le grandi organizzazioni dispongono di ingenti risorse per ripristinare servizi e sistemi dopo eventi di natura cibernetica, dall'altro, le PMI, con disponibilità non altrettanto elevate, potrebbero trovarsi costrette a doversi confrontarsi con tali forme innovative di estorsione.

Per illustrare meglio il concetto di "cyber pizzo" potrebbe essere opportuno approfondire tre aspetti: la territorialità della minaccia, l'eterogeneità degli attaccanti, la certezza della protezione a seguito del pagamento.

[8] https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes

Per quanto riguarda il primo aspetto, ovvero la territorialità della minaccia, le eventuali dinamiche legate a tali fenomeni si devono necessariamente confrontare con le peculiarità della dimensione cyber che, per propria natura, risulta essere a-territoriale, ovvero de-territorializza attaccanti e vittime nello spazio cibernetico. Le vittime, pertanto, risultano potenzialmente bersagli a prescindere dalla loro posizione geografica consentendo anche ad attori malevoli provenienti da altri stati di realizzare l'offensiva nei confronti di PMI nazionali. Inoltre, la totale assenza di definiti legami con il territorio potrebbe aumentare la complessità delle attività di intelligence in relazione alla minaccia, inasprendo finanche la difficoltà di indagine delle Autorità deputate alla sicurezza in ambiente cyber. Questo aspetto dà luogo, inoltre, a una pronunciata eterogeneità degli attaccanti che, non essendo limitati dalla dimensione territoriale, possono avere caratteristiche estremamente diverse in termini di modus operandi, competenze tecniche, dimensioni e finalità. A titolo di esempio una PMI potrebbe essere attenzionata nello stesso periodo sia da un gruppo hacker state sponsored operante in ambiente internazionale, sia da soggetti singoli, non inseriti in realtà organizzate e con poca esperienza alle spalle.

In merito al terzo aspetto, analogamente a quanto avviene per il "pizzo" tradizionale della criminalità organizzata, nelle ipotetiche dinamiche della controparte cyber non vi sarebbe alcuna certezza rispetto all'ottenimento di una protezione concreta da parte degli attaccanti, a seguito di un pagamento di natura economica. Tale incertezza risulta ragionevole anche analizzando i comportamenti degli attaccanti dopo la realizzazione di attacchi malware di tipologia ransomware, in cui generalmente viene richiesto un riscatto economico per il ripristino dei sistemi attaccati. Infatti, non è raro che, come suggerito dallo studio condotto da Cybereason[9], le vittime, dopo aver effettuato il pagamento, vengano nuovamente bersagliate dallo stesso attaccante. Tale fenomeno testimonierebbe l'alta inaffidabilità degli attaccanti che si muovono nella dimensione cyber, presumibilmente generata dalla natura virtuale e dalla conseguente assenza di "fisicità" degli attori coinvolti.

4. Le ricadute delle norme di cyber security sulle PMI italiane

Il decreto legislativo di recepimento della direttiva NIS e la legge 133/2019 hanno dato luogo alla realizzazione di due liste di aziende identificate rispettivamente come OSE, Operatori di Servizi Essenziali e come OSF, Operatori di Servizi Fondamentali. Entrambe le liste sono classificate per evidenti motivi di sicurezza e sono dinamiche, nel senso che potranno essere aggiornate nel tempo.

È evidente che alcune PMI sono parte di entrambe le liste, tuttavia la ricaduta principale non è legata tanto alla diretta appartenenza a tali categorie, ma soprattutto alla supply chain.

Entrambe le norme e soprattutto il PSNC, infatti, impongono una serie di adempimenti, i quali non possono essere rispettati se non si aggancia a un comportamento virtuoso

[9] https://www.cybereason.com/blog/three-reasons-why-you-should-never-pay-ransomware-attackers

e virtuosamente sicuro anche la supply chain, quanto meno per i fornitori di servizi critici, ovvero collegati ai servizi interni al Perimetro stesso.

I decreti attuativi del Perimetro prevedono una serie di controlli da applicare alla supply chain e, in ogni caso, tutti gli appartenenti alla lista del PSNC stanno già lavorando per stringere contratti con i fornitori critici più attenti ai requisiti di sicurezza. Molti di questi fornitori critici sono PMI che risultano quindi fortemente interessate da quanto previsto nelle norme, seppur indirettamente e con un ritardo temporale dipendente dal tipo di fornitura, dal cliente e dai margini negoziali di quest'ultimo rispetto alle richieste legate ai requisiti di sicurezza.

Ci aspettiamo, quindi, un incremento dell'attenzione alla cyber security da parte delle PMI direttamente o indirettamente proveniente dall'applicazione del PSNC. Questa maggiore attenzione dovrà necessariamente comportare alcuni investimenti in sicurezza rispetto ai quali il mercato delle PMI non sembra avere chiarezza e, tanto meno, determinazione.

Un altro aspetto interessante sarà legato a possibili obblighi di certificazione di prodotto, soprattutto per le PMI che lavorano su servizi legati al 5G e alle sue applicazioni. Questo tema dovrà comunque essere affrontato di pari passo con i produttori della tecnologia e non ci aspettiamo che determini un'attenzione maggiore a buone pratiche di cyber security.

La Agenzia per Cyber security Nazionale promulga la sovranità nazionale in tema digitale. Una sovranità hard implica una capacità autonoma di produzione che copra tutto il flusso della catena del valore, comprese materie prime e logistica, comprese le fonderie dei microchip e non può che essere contestualizzata a livello regionale europeo. Esiste poi una sovranità digitale "soft" che considera il capitale umano. Qui il perimetro è molto chiaro secondo la ACN, è prettamente italiano e richiama addirittura cervelli dall'estero con la promozione di un "corridoio di rientro" per i nostri laureati.

Purtroppo, però, l'attuale situazione del mercato del lavoro della cyber security si può accomunare alla situazione artistica del Rinascimento italiano: le grandi aziende premono giocano al rialzo continuo degli stipendi, di fatto "rubandosi" l'un l'altra gli esperti. Ma un fenomeno di mecenatismo non è la risposta alle istanze di cyber security di questo tempo: esso esclude tutte le PMI dalla possibilità di permettersi personale con competenze cibernetiche. Se non iniziamo a produrre cervelli, anche mediocri, in tema di cyber security, questa disciplina resterà preda del mecenatismo e quindi un privilegio di pochi.

5. Conclusioni

Lo scenario descritto evidenzia come le PMI si trovino attualmente di fronte a nuove sfide legate alla costante evoluzione del ruolo ricoperto dalla dimensione cibernetica, accelerata anche dall'insorgenza e dalla diffusione della pandemia Covid-19. L'analisi del panorama normativo europeo e nazionale mette in luce il recente interesse delle istituzioni governative verso la tematica della sicurezza informatica, considerata ormai elemento fondamentale per il funzionamento del sistema-Paese e dell'Unione europea. I cambiamenti normativi in atto dimostrano, inoltre, una consapevolezza del legislatore di dover garantire un

costante aggiornamento del corpus normativo di settore ai fini di intercettare le più recenti dinamiche. I casi della NIS2 e della CER, attualmente ancora in discussione, rappresentano dei validi esempi di tale consapevolezza a livello europeo. Dal punto di vista nazionale i recenti sforzi per la concretizzazione del Perimetro di Sicurezza Nazionale Cibernetica e l'istituzione dell'Agenzia per la Cybersicurezza Nazionale si configurano come pietre miliari della nuova architettura nazionale di sicurezza cibernetica, volte a garantire presidi di sicurezza adeguati alle nuove sfide. Tuttavia, la concreta applicazione di quanto previsto dall'apparato normativo sinora costruito, nelle realtà di piccola e media dimensione, resta una sfida aperta. Tale complessità si unisce alle esigue risorse impiegate da queste realtà nella formazione del personale e nell'inserimento di risorse qualificate. Con questi presupposti non è da escludere l'ipotesi di comparsa di forme estorsive con logiche similari al "pizzo" della criminalità organizzata traslate nella dimensione cyber. Tale fenomeno, potenzialmente concretizzabile attraverso differenti metodi, potrebbe configurare scenari particolarmente critici per le PMI, aumentando il livello di rischio cibernetico a cui esse sono esposte.

In questo senso assumono una particolare rilevanza strumenti di riduzione della complessità messi a disposizione liberamente da esperti di settore provenienti dal mondo accademico nonché da realtà pubbliche e private. A titolo di esempio si evidenzia il recente contributo, in fase di pubblicazione, dell'Associazione Italiana esperti in Infrastrutture Critiche (AIIC) circa l'evoluzione del quadro normativo europeo e italiano in materia di cybersecurity. Tale lavoro, disponibile sul sito dell'Associazione, consiste in un testo volto a raccogliere e sintetizzare tutte le normative europee e nazionali riguardanti la sicurezza cibernetica. Grazie a tale contributo si potrà disporre di una nuova visione d'insieme delle norme di settore, con approfondimenti riguardanti l'ambito di applicazione di ciascuna di esse, i settori interessati e le eventuali sanzioni previste.

Bibliografia

[1] Clusit - Rapporto 2021 sulla Sicurezza ICT in Italia.
[2] Relazione 2020 sulla politica dell'informazione per la sicurezza.
[3] DIS - Documento di sicurezza nazionale 2020, Allegato alla Relazione annuale al Parlamento ai sensi dell'art. 38, comma 1 bis, legge 124/2007.
[4] DIRETTIVA (UE) 2016/1148 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 6 luglio 2016 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.
[5] Decreto-legge 21 settembre 2019, n. 105: "il danno o pericolo di danno all'indipendenza, all'integrità o alla sicurezza della Repubblica e delle istituzioni democratiche poste dalla Costituzione a suo fondamento, ovvero agli interessi politici, militari, economici, scientifici e industriali dell'Italia, conseguente all'interruzione o alla compromissione di una funzione essenziale dello Stato o di un servizio essenziale".
[6] CIS-Sapienza, CINI Cybersecurity National Lab, Framework Nazionale per la Cybersecurity e la Data Protection, febbraio 2019.

[7] https://www.yarix.com/wp-content/uploads/2021/04/Cybersecurity-e-data-protection-levoluzione-del-contesto-e-lo-scenario-....pdf (ultimo accesso Febbraio 2022)
[8] https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes (ultimo accesso Febbraio 2022)
[9] https://www.cybereason.com/blog/three-reasons-why-you-should-never-pay-ransomware-attackers (ultimo accesso Febbraio 2022)

Biografie

Luisa Franchina, cofondatore e presidente di AIIC, attualmente ricopre il ruolo di Partner e COO di Hermes Bay. Già Direttore Generale della Segreteria per le Infrastrutture Critiche (Presidenza del Consiglio dei ministri 2010-2013) ha ricoperto diversi incarichi nel settore della Pubblica Amministrazione e nel settore privato. Ha pubblicato numerosi articoli e libri sulla sicurezza e sulla protezione delle infrastrutture critiche.

Andrea Lucariello è Area Director e Senior Consultant presso Hermes Bay, si occupa di Cyber Security, Cyber Governance, Cyber Threat Intelligence e di Enterprise Risk Management. Fornisce supporto, in qualità di DPO, in ambito di protezione dei dati personali. Auditor/Lead Auditor ISO 27001:2017 – 22301:2019. Dal 2020 è Security Manager ai sensi della UNI 10459:2017.

Alessandro Calabrese. Laureato in Linguistica computazionale presso l'Alma Mater Studiorum Città di Bologna, con un master in Sicurezza e Intelligence presso Link Campus University. Attualmente lavora presso Hermes Bay come Senior Consultant e Area Director nell'ambito di Enterprise Risk Management, Cyber Security e Cyber Governance.

Francesco Ressa. Laureato in Scienze Politiche alla LUISS Guido Carli e Master in Sicurezza Informatica e Informazione Strategica presso la Facoltà di Ingegneria dell'informazione, informatica e statistica della Sapienza di Roma. Lavora come Area Director e Senior Consultant presso Hermes Bay in materia di Enterprise Risk Management, Cyber Security e Cyber Governance.

Art Attach – Il mondo digitale con il linguaggio dell'arte

Le relazioni, tra estetica e digitale

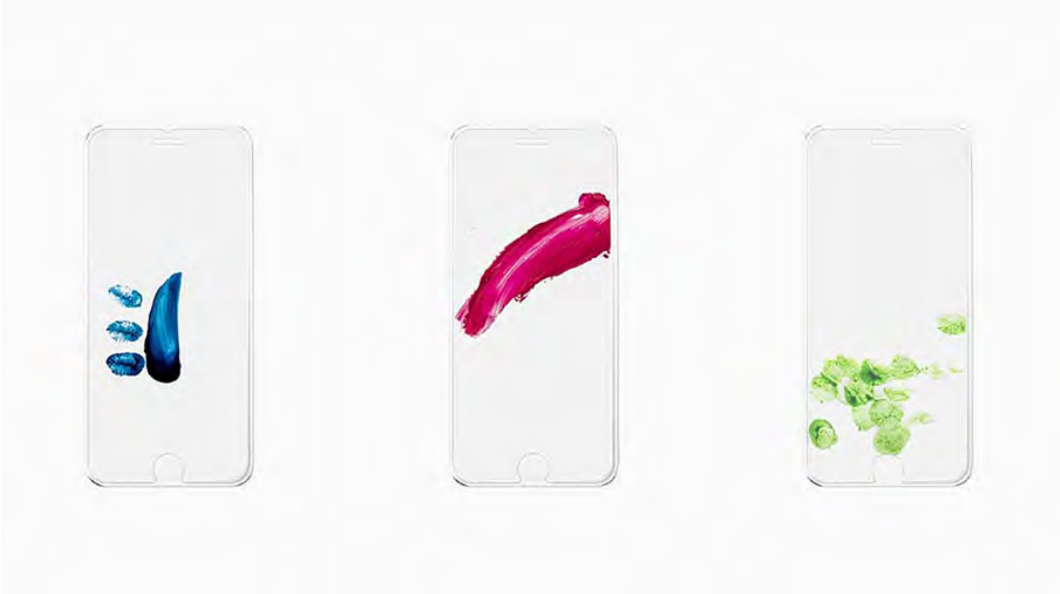
Silvia Crafa

Quando si parla di software si intende in generale un qualsiasi programma informatico. Ma la natura dei programmi è molto variegata: si va ad esempio da un software di videoscrittura su computer, ad un intreccio di applicazioni (un sistema software) che gestisce i dati digitali di un ospedale; è un software anche ciò che definisce l'aspetto e il comportamento di una pagina web, o un algoritmo che definisce un motore di ricerca, o ancora il sistema operativo che gestisce il funzionamento di uno smartphone. Ma un modo interessante e molto generale di concepire il software consiste nel vederlo come uno **strumento di mediazione** [1,2,3]. Infatti chi progetta un software definisce in modo preciso e non ambiguo non solo la funzionalità del programma in questione, ma anche quali sono gli (unici) input a cui reagisce il programma, e qual è il tipo di output che viene prodotto. Ad esempio, costruire una pagina web che contiene testo norvegese significa restringere l'insieme degli utenti a coloro che sono in grado di leggere e inoltre conoscono la lingua norvegese. Analogamente, fornire i risultati di una ricerca online sotto forma di un elenco ordinato di risultati, impone una gerarchia di tali risultati, determinando così una priorità o una vera e propria scala di rilevanza. Tutte queste scelte nella progettazione del software si rivelano, esplicitamente o implicitamente, forme non neutrali di mediazione tra il software e il suo contesto d'uso.

L'analisi dei prodotti software come strumenti di mediazione offre moltissimi spunti, vogliamo qui approfondirne un particolare aspetto: quale tipo di **relazione** si crea tra un sistema digitale e chi lo usa, gettando lo sguardo lì dove

una persona produce un input oppure interpreta o raccoglie un output. Per farlo cerchiamo di usare il linguaggio dell'arte, che ha certamente una speciale capacità di cogliere e osservare le relazioni.

Ricordiamo che i lettori sono invitati ad intervenire nella discussione segnalandoci le loro impressioni e le opere che li hanno ispirati, scrivendo a artattach.mondodigitale@aica. Noi intanto ci soffermiamo su due opere del giovane artista italiano Guildor (https://www.guildor.com/), e ci facciamo aiutare da Marcello Ghilardi, professore di estetica presso l'Università di Padova.



Silvia Crafa: Nell'opera "I'll meet you across the surface" (Guildor, https://www.guildor.com/ill-meet-you-across-the-surface/) l'autore cattura con dei colori acrilici la navigazione gestuale di alcune app di social media. Si tratta di gesti compiuti inconsciamente centinaia di volte, rappresentano il confine tra la persona e l'applicazione, e materializzano il vero e proprio input atteso dal software. Anche il titolo dell'opera richiama l'attenzione su questa soglia, dove la continuità fisica dell'intenzione e del dito della persona si trasforma in input digitali scelti da un insieme predefinito dal progettista software.

Prof. Ghilardi, nel mondo dell'arte il gesto è un tema ricorrente; che significato o che valore ha catturare un gesto?

> Marcello Ghilardi: La questione del **gesto** (inteso come singolo atto intenzionale e significante) e della gestualità in generale (che intenderei come la dimensione complessiva, o la condizione di possibilità che permette l'attivarsi di innumerevoli singoli gesti nelle nostre vite umane) è di capitale importanza per provare a pensare l'esperienza umana, le sue forme espressione, l'intreccio tra aspetti corporeo-percettivi, artistici e interattivi nei confronti del mondo che ci circonda. Pensare "il gesto" significa rendersi conto che non si dà mai un corpo in sé, astratto, che

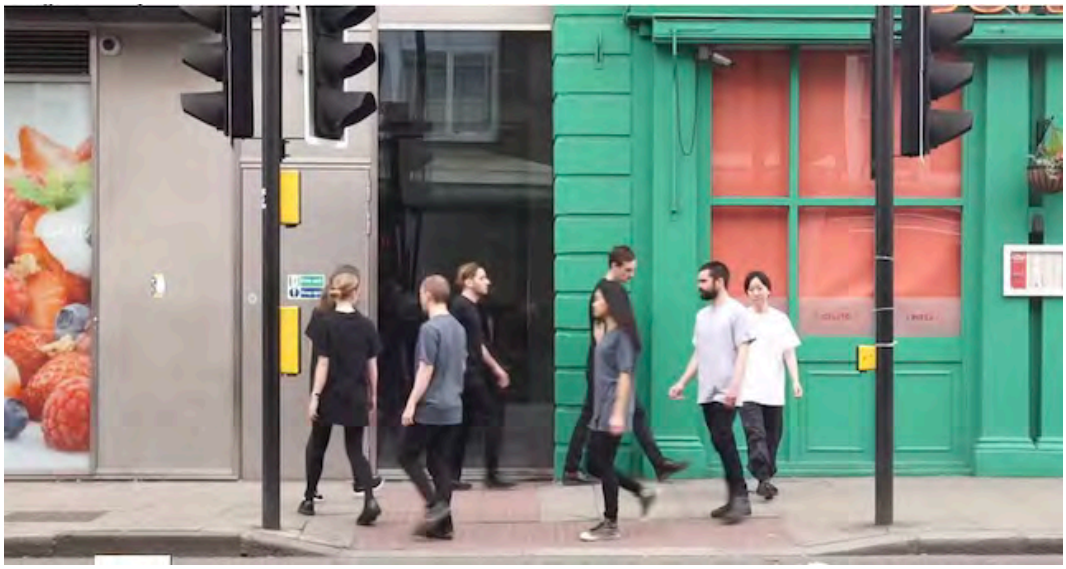
solo in un secondo tempo si attua eventualmente in un gesto o in un altro gesto; significa invece capire che il corpo è sempre in situazione, in atto. Perfino il sonno, per quanto non sia una condizione paragonabile, per esempio, a un atto deciso e consapevole come l'esecuzione di una sonata al pianoforte, è comunque una situazione in cui il corpo si dispone a una serie di gesti o di atti che lo definiscono e lo circoscrivono. Ciò implica una conseguenza importante, ovvero il fatto che l'identità psicofisica dell'essere umano è sempre in relazione, anzi: è relazione, più che sostanza (una sostanza che se ne sta per conto suo e che occasionalmente entra in relazione, compie dei gesti, poi di nuovo rimane ferma e zitta, avulsa dal contesto).

SC: Molto interessante: quindi anche i gesti sulla superficie dello smartphone non sono solo qualcosa che noi eseguiamo, ma sono parte di noi, nel senso che quei gesti, cioè quella specifica forma di relazione con lo smartphone, contribuisce a dire chi siamo.

Anche l'idea di **soglia** qui è rilevante: la superficie dello smartphone è un punto di traduzione tra due linguaggi, il gesto umano e l'input di un software artificiale. Nella nostra abituale fusione con lo smartphone abbiamo perso la percezione del confine e della soglia, e di conseguenza anche del filtro e della mediazione che essa implementa.

MG: Anche la nozione di "soglia" è particolarmente efficace per dire la relazionalità in cui siamo immersi, perché per definizione una soglia connette un qui e un là, un esterno e un interno, un prima e un poi. Un aspetto interessante delle soglie e dei confini è che al tempo stesso legano e distinguono, uniscono e disgiungono; non sono né di là né di qua, e proprio perciò permettono la formazione di un "qua" e di un "là". La nostra vita è continuamente determinata da soglie, fisiche (la nostra pelle, la porta di casa, l'ingresso della scuola, di uno spazio sacro…) e temporali (la nascita, il battesimo, il primo giorno di scuola, la laurea, la nascita di un figlio, la morte). Una soglia, intesa anche come interfaccia, è un punto-limite in cui universi apparentemente distanti entrano in contatto e comunicano, tanto che il nostro corpo – grazie alla dinamica dei partitori di tensione nel caso della tecnologia touchscreen – può interagire con zone "sensibili" di uno smartphone. La soglia che è la mia pelle (l'involucro che per abitudine pensiamo costituisca grosso modo il limite fisico della mia persona) entra in contatto con la soglia/superficie sensibile del telefono o del tablet e produce una serie di effetti, modificando per esempio la mia interazione con il mondo e con gli altri o producendo stimoli ed emozioni (per esempio se tocco un video di YouTube che trovo particolarmente interessante e commovente). Mi piace ricordare che un software è, almeno per ora, tendenzialmente una scrittura eseguita da altri esseri umani, e tramite la mediazione di una "soglia" tecnologica l'utente entra virtualmente in contatto (pur senza saperlo, in genere) con quella scrittura

e quelle idee che si sono “tradotte” nel linguaggio di programmazione del software. Facendo eseguire a un determinato programma i suoi compiti, l’utente riesce effettivamente a ottimizzare il proprio lavoro, in molti casi, o può divertirsi un mondo, ma raramente è consapevole che quei programmi già declinano in un certo modo il suo lavoro, indirizzano e determinano in un certo modo il suo divertimento. Accedere a una soglia e varcarla dovrebbe sempre, possibilmente, essere un gesto consapevole, libero dall’illusione che il medium o lo strumento di cui ci serviamo siano neutri.



SC: Nella performance “IRL is what happens to you while your life is busy buffering” (Guildor - https://www.guildor.com/irl-is-what-happens-to-you-while-your-life-is-busy-buffering/) gli attori aspettano la luce verde del semaforo pedonale impersonando la tipica icona software che, tramite una rotella che gira, rappresenta il segnale che l’utente deve attendere la terminazione del processo di caricamento dei dati (buffering).

IRL è un acronimo usato nelle piattaforme social, significa ”In Real Life” e gli streamer IRL sono coloro che si riprendono durante le proprie azioni quotidiane e postano questi contenuti online, spesso realizzando numerosissime visualizzazioni. Dunque il titolo dell’opera sottolinea il **ribaltamento tra l’online e l’IRL**: è la nostra vita che è in momentaneamente in stand-by, in attesa di completare il buffering, “il caricamento” di un prerequisito necessario al proseguimento dell’azione, e gli attori materializziano l’online dando vita all’icona software dell’attesa.

MG: È vero che la separazione tra mondo “reale” e mondo “virtuale” rischia di essere fittizia e incapace di “leggere dentro” (intus-legĕre, che è la prestazione propria dell’intelligenza) il nostro modo di abitare il mondo e

la tecnologia. La scheggia di selce per il nostro antenato che tagliava un pezzo di carne, il bastone per il cieco, il violino per il violinista non sono semplici strumenti che si aggiungono al corpo, ma diventano un'estensione del corpo, delle protesi che permettono una relazione diversa e aumentata della nostra identità con il mondo di cui siamo parte (e che non è semplicemente un ambiente in cui noi ci muoviamo, perché esso ci determina e noi lo plasmiamo, in un rapporto molto più biunivoco e simbiotico di una mera relazione di inclusione). Analogamente, le tecnologie digitali diventano oggi per noi protesi psico-fisiche, che ci consentono di estendere la nostra presenza in suono e immagine dall'altra parte del mondo, dove vive l'amico lontano, oppure ci fanno vivere emozioni e provare sentimenti interagendo con un joypad e vivendo avventure digitali, che possono poi avere effetti di realtà, con strascichi di umore anche molto importanti (come sanno bene i genitori di figli adolescenti appassionati di videogames). Ma se mondo reale e mondo virtuale non possono e probabilmente non devono essere nettamente "separati", tuttavia non è detto che non debbano venire "distinti". La distinzione non è la separazione; mentre quest'ultima in effetti non accade, non si dà, per la continuità psichica che sussiste tra questi universi, è cruciale capire e tenere presente la loro distinzione, per evitare di pensare che il virtuale (in senso digitale) sia un prolungamento senza soluzione di continuità del mondo fisico, o che la mia identità virtuale (in un social network) possa sovrapporsi e ricoprire o addirittura annullare la mia identità psicofisica, che invece resta legata anche al hardware, cioè il nostro corpo, con tutta la stanchezza, la fatica, ma anche la gioia e l'esuberanza che talvolta ci fa avvertire.

SC: Infine, questa performance ci interroga sul nostro modo di percepire il tempo, sul disagio che proviamo duranti i tempi morti, e sul senso di impazienza che i dispositivi digitali hanno in noi accresciuto. La tecnologia da sempre media la nostra **relazione con il tempo**, e la pervasività delle app digitali ha disgregato anche la continuità della nostra attenzione. Avvertiamo così tutta la difficoltà di stare nel tempo morto, sentendo l'urgenza di riempire il vuoto, non tanto con un contenuto, ma anche solo con un movimento. L'icona software che indica l'attesa sarebbe meno efficace se fosse una rotellina ferma: renderebbe l'utente ancora più impaziente. Il disagio infatti non sembra venire dall'assenza di contenuto ma dall'interruzione del movimento, del flusso continuo di stimoli esterni; per questo dà sollievo anche camminare inutilmente in cerchio in attesa del semaforo verde, l'importante è non bloccarsi in uno stato di stasi.

Vorrei concludere con delle suggestive riflessioni di Alessandro Baricco: "dove la distinzione tra mondo vero e mondo virtuale decade a confine secondario, dato che l'uno e l'altro si fondono in un unico movimento che genera, nel suo complesso, la realtà. […] un millennial considera le macchine un'estensione di se stesso, non un qualcosa che media il suo rapporto con le cose. Uno smartphone non è diverso per lui da un paio di scarpe o uno stile di vita. Le macchine per lui non sono mediazioni. Sono articolazioni del suo stare al

mondo.[…] Ciò che accade tende a farlo, per esistere veramente, con la forma di una traiettoria, di rado con la compostezza di un punto: sempre più spesso non ha un inizio, non ha una fine, e il suo senso è scritto nella traccia cangiante che lascia dietro di se´"[A. Baricco, The Game, 2018].

Quindi, se da un lato il software è sempre uno strumento che media le nostre relazioni, con il tempo, con il corpo, con la nostra vita, dall'altro questo ruolo di mediatore è sempre più invisibile, più impercettibile. Forse perché questo ruolo è dato sempre più per acquisito e scontato, o forse perché le soglie sono sempre più progettate per essere invisibili.

Bibliografia

[1] I. van de Poel, L. Royakkers. Ethics, Technology and Engineering. Wiley-Blackwell ed. 2011.

[2]L. Winner. Do Artifacts Have Politics? Daedalus, 109(1), 121–136. (1980) Available at http://www.jstor.org/stable/20024652

[3] S. Crafa. Dalle competenze alla consapevolezza digitale: capire la complessità e la non neutralità del software. In "Etica, Diritto e Tecnologia", a cura di P. Moro. Edizioni Franco Angeli, 2021.

Introduzione all'articolo di Anna Vaccarelli per la rubrica "Ada e le altre"

Francesca Alessandra Lisi

Se vi è un settore dell'informatica attuale in cui la figura stereotipata dell'hacker (come giovane maschio bianco con l'immancabile felpa col cappuccio) appare con maggior evidenza a popolare l'immaginario comune, quello è il settore della cybersecurity. Il che spiega l'inevitabile allontanamento della popolazione femminile dal settore, persino più marcato che in ICT nel suo complesso.

Ce ne parla in questo numero Anna Vaccarelli, Dirigente Tecnologo presso l'Istituto di Informatica e Telematica del CNR e co-fondatrice della community Women for Security. L'intento della community è di sfatare falsi miti, scardinare stereotipi, al fine di avvicinare le ragazze al mondo della cybersecurity, mediante azioni di comunicazione, sensibilizzazione e di orientamento.

Dati alla mano, Vaccarelli ci aiuta ad analizzare il problema della sottorappresentazione femminile nel settore. E ci conferma l'importanza per le donne di "fare rete", per valorizzare il proprio contributo scientifico e tecnologico, e per incoraggiare quelle più giovani. I crescenti attacchi alla sicurezza dei nostri sistemi informatici richiedono infatti anche un numero sempre più nutrito di cyber ladies.

Women for Security: una community dedicata alle cyber ladies italiane

Anna Vaccarelli

Parità di genere, gender gap, pari opportunità: tutti termini che sempre più spesso appaiono nei nostri discorsi, sui media, nelle interviste a politici e opinion makers. Vengono riferiti a vari ambiti sociali e lavorativi, ma nel settore delle cosiddette STEM (le discipline *Science, Tecnology, Engineering, Mathematics)* il dibattito è particolarmente vivace: la differenza di presenza tra donne e uomini in questo campo è significativamente marcata.

Se si guarda più nel dettaglio il settore dell'ICT il divario si accentua. Il rapporto DESI [1] indica quasi 19% di donne impiegate nel settore ICT in Europa; per l'Italia la percentuale scende al 16% [2]. Il rapporto AlmaLaurea 2021 [3] rivela che nei corsi di Laurea le donne sono una minoranza nei gruppi informatica e tecnologie ICT (14,3%) e ingegneria industriale e dell'informazione (25,9%).

I dati sulle donne nella cybersecurity indicano una presenza ancora minore rispetto al settore ICT in generale: secondo il rapporto di ICS^2 [4] oggi, in tutto il mondo, le donne nel settore della cybersecurity sono solo il 24% della forza lavoro, ma spesso nei ruoli manageriali la percentuale supera quella degli uomini, così come è più alta la percentuale di donne con una formazione post laurea (52%) contro il 44% degli uomini; circa la metà del campione (45%) sono millenials, mentre per gli uomini ci si ferma al 33%. Questo dato si ribalta per la generazione X: il 44% degli uomini vs il 25% delle donne.

I motivi posso essere molti: primo fra tutti la convinzione che quella della cybersecurity non sia una professione o un settore adatto a una donna. A questa convinzione contribuisce lo stereotipo dell'esperto di cybersecurity che viene normalmente proposto: maschio, solitario di fronte al suo computer, in uno scenario tipicamente blu scuro, un po' cupo e misterioso, come dimostra la maggior parte delle immagini che si trovano sui motori di ricerca con la parola chiave "esperto cybersecurity" [5]. Non meno importante è il fattore della formazione scolastica o dell'educazione familiare, che non contribuisce

favorevolmente a indirizzare le ragazze verso questo ambito di lavoro e conoscenza: ancora oggi le ragazze vengono indirizzate verso professioni più orientate ai settori umanistici o di scienze della vita e che, possibilmente, lascino tempo per le cure familiari, storicamente “appaltate” alle donne.

È su questi dati e questi fatti che - con un piccolo gruppo di donne impegnate nel settore della cybersecurity - ci siamo trovate a riflettere quasi due anni fa, in piena pandemia: abbiamo concluso che non bastava parlarne, bisognava agire, trovarsi insieme e collaborare. Da questa determinazione è nata l'idea di far nascere una community italiana di donne coinvolte nel settore della cybersecurity, le **Women for Security**, dove ci fosse spazio per il confronto, la consapevolezza e le iniziative di “sostegno” e incoraggiamento per altre donne. Volevamo anche che fosse un’occasione per affermare la nostra presenza in questo settore davanti ai numerosi uomini e ai decisori (quasi sempre maschi). Cinzia Ercolano, Cristina Gaia e Carmen Palumbo sono state le promotrici e, a partire dal 2020, si sono aggiunte altre "colleghe" (tra cui me, della qual cosa sono molto onorata).

Oggi la community conta quasi duecento professioniste, che condividono i valori su cui si fonda Women for Security: Competenze, Condivisione e Crescita. Il clima che si respira tra le cyber ladies non è competitivo, ma di comprensione, complicità e solidarietà. Lo spirito è sempre costruttivo, propositivo e concreto, volto a intraprendere iniziative con l’obiettivo di ottenere i risultati prefissati, con determinazione. Ciascuna di noi collabora e mette a disposizione le proprie competenze a livello volontario, proprio nello spirito di condividere e crescere insieme: la pragmaticità, la capacità di analisi ed il diverso punto di vista dell’universo femminile apportano un valore aggiunto.

Le nostre competenze vengono da esperienze lavorative diverse: siamo ricercatrici, ricopriamo profili tecnici o legali, lavoriamo nel settore della comunicazione e del marketing, o nelle vendite, ma sempre nell’ambito della cybersecurity. Questo è il primo messaggio che vogliamo far passare: lavorare in questo settore non implica necessariamente di essere hacker!

Come Women for Security vogliamo contribuire a diffondere la cultura della cybersecurity anche verso le fasce più giovani della popolazione: per esempio, con iniziative di formazione e orientamento, per incoraggiare le giovani donne ad abbracciare le discipline STEM e le nuove professionalità che evolvono con l’evoluzione tecnologica e digitale. Inoltre, nel settore della cybersecurity la domanda di esperti è molto maggiore dell’offerta, indipendentemente dal fattore sesso: è un aspetto che cerchiamo di sottolineare molto per invogliare le ragazze (ma in generale tutti i giovani) a formarsi in questo settore. È proprio a causa della carenza di competenze e figure professionali a livello globale che oggi la cybersecurity è un’emergenza.

In questa ottica partecipiamo a eventi divulgativi, soprattutto se rivolti a studentesse e studenti, come per esempio il laboratorio interattivo, che abbiamo svolto a Internet Festival nel 2021 e che ripetiamo a ottobre nel 2022, la Fastweb Digital Academy 99eLode, i corsi per l’Associazione Italiana Traduttori e Interpreti, solo per citarne alcuni. Ci sforziamo di creare awareness sia nei nostri

ambiti lavorativi di origine che in contesti pubblici di eventi e iniziative ai quali partecipiamo.

È importante lavorare e progettare le attività avendo un'idea reale dello scenario e delle esigenze e lo facciamo attraverso delle survey. In questi due anni di attività abbiamo lanciato due survey: una sul **revenge porn** e una sulle **donne nella cybersecurity**. Per la prima survey abbiamo collezionato oltre 500 risposte in poche settimane, raccogliendo esperienze, pareri e suggerimenti dai rispondenti, sia maschi che femmine. Per la seconda [7] abbiamo raccolto oltre 200 risposte in circa 10 mesi, segno evidente che le donne inserite nel settore della cybersecurity sono poche e non è facile intercettarle. I risultati, tuttavia, sono stati molto interessanti: sono prevalentemente millennials (come per ICS^2), oltre la metà delle rispondenti è laureata (55%), mentre un terzo (31%) ha conseguito una formazione post-laurea; la maggior parte delle professioniste (44%) lavora nell'ambito tecnico della cybersecurity e solo il 5% ricopre una funzione dirigenziale C-Level (CEO, CIO, COO, CTO, …). Il 39% afferma di aver avuto una carriera più lenta degli uomini, il 34% sostiene parità e per un 6% è stata più veloce. Il tasto dolente resta quello del carico del lavoro familiare: per il 48% è un problema e solo il 23% ritiene che sia ugualmente ripartito. È confortante sapere che circa la metà del campione ritiene di godere della stessa considerazione dei colleghi maschi (48%) e che lavorare in un ambiente prevalentemente maschile non ha costituito un problema (92%). Infine abbiamo cercato di capire quali siano le esigenze e le azioni più efficaci da intraprendere per incoraggiare le donne a lavorare nel campo della Cyber Security e riuscire nel tempo a colmare il gender gap.

Le opzioni vincenti sono:

- le campagne di sensibilizzazione sull'importanza e l'impatto della cybersecurity sulla società e sulle esigenze di mercato e le opportunità lavorative che il settore offre
- l'attività di mentoring da parte di professioniste esperte, così come le azioni di promozione da parte delle Università
- le azioni da parte del Governo verso le studentesse delle scuole secondarie di primo e secondo grado

Rispetto al primo e al secondo punto pensiamo di poter dare un contributo, mentre il terzo richiede un intervento "strutturale" sulle scuole. Amplieremo la nostra attività di divulgazione e di consapevolezza della cybersecurity anche attraverso pubblicazioni dedicate e attraverso la creazione, al nostro interno, di tavoli tecnici che ci aiutino a mettere a fuoco e a sviluppare temi specifici. A ciascun tavolo invitiamo le cyber ladies con l'esperienza più adatta e vicina al tema scelto. Ci rendiamo da sempre disponibili ma ci proporremo anche attivamente come "role model" e "mentori" nei contesti che vedono coinvolti i giovani e soprattutto le ragazze, come è già successo, per esempio, nel caso della nostra partecipazione al Cyber Trials 2022, organizzato dal CINI.

Riferimenti

[1] Rapporto Desi 2021 Europa https://digital-strategy.ec.europa.eu/en/policies/desi

[2] Rapporto Desi 2021 Italia, https://digital-strategy.ec.europa.eu/en/policies/desi-italy

[3] XXIII Indagine profilo dei Laureati 2020, Report 2021, Consorzio Interuniversitario AlmaLaurea

[4] https://www.isc2.org/-/media/ISC2/Research/ISC2-Women-in-Cybersecurity-Report.ashx

[5] https://code.likeagirl.io/why-is-there-a-lack-of-women-in-cyber-667ce7fae6e7 e https://www.redhotcyber.com/post/perche-mancano-le-donne-nel-cybersecurity/

[6] Rapporto Eurostat https://ec.europa.eu/eurostat/statistics-explained/index.php?title=ICT_specialists_in_employment - ICT_specialists_by_sex

[7] https://womenforsecurity.it/dettaglio/58