

www.ictedmagazine.com



INFORMATION COMMUNICATION TECHNOLOGIES EDUCATION MAGAZINE

PERIODICO DELLE TECNOLOGIE DELL'INFORMAZIONE E DELLA COMUNICAZIONE PER L'ISTRUZIONE E LA FORMAZIONE

EDITORIALE

Il Tempo nell'era digitale

GENERAZIONI A CONFRONTO

Sfruttamento sessuale on line dei minori

DIDATTICA E TECNOLOGIE

L'intelligenza artificiale nella scuola di base: uno studio dell'Università della Finlandia Orientale.

LAVORO E SICUREZZA

Robotica collaborativa

ROBOTICA E PENSIERO COMPUTAZIONALE

Pensiero computazionale: imparare a sviluppare strategie fin da bambino

SICUREZZA INFORMATICA

Lo spear phishing e l'utilizzo di nuove tecniche con la social engineering

ANNO IV - N.4 - GENNAIO 2022



ICTEDMAGAZINE

Information Communication Technologies Education Magazine

Periodico delle Tecnologie della
Comunicazione e dell'Informazione per
l'Istruzione e la Formazione
Registrazione al n.157 del Registro Stampa presso il
Tribunale di Catanzaro del 27/09/2004
ISSN 2611-4259 ICT Ed Magazine (on line)

Rivista trimestrale

Anno IV- N° 4 - Gennaio 2022
Data di pubblicazione Gennaio 2022
Via Pitagora, 46 – 88050 Vallefiorita (CZ)

Direttore Editoriale

Editore-responsabile intellettuale

Luigi A. Macri
direzione@ictedmagazine.com

Editing e revisione editoriale

Maria Brutto

Redazione

Claudia Ambrosio
Maria Brutto
Benedetto Fucà
M. F. Oraldo Paleologo
Paolo Preianò
Davide Sorrentino
Rosa Suppa

Hanno collaborato

Mario Catalano
Andrea Cortese
Massimiliano Nespola
Ludovica Zoccali

Webmaster

Rocco Voci - Synapsis

Impaginazione

Manuela Gaetano - CSV Calabria Centro

Grafica

I.I.S. "Pertini-Santoni" - Crotone
Dirigente - Ida Sisca
Grafic Designer - Franco Nicotera

ICTEDMagazine è un periodico trimestrale, in formato digitale, delle tecnologie dell'informazione e della comunicazione per l'istruzione e la formazione; un progetto editoriale che vede impegnati docenti, genitori, tecnici, esperti e professionisti delle diverse categorie del sapere. Il nostro obiettivo è di contribuire a migliorare la consapevolezza dei genitori e della Società tutta, relativamente alle problematiche legate all'uso delle tecnologie con particolare attenzione ai minori, agli studenti, ed a tutti coloro che vivono una condizione sociale debole. Vengono, inoltre, trattati temi che riguardano la sicurezza e la protezione del proprio computer dai continui attacchi esterni nonché indicazioni a docenti e studenti su tematiche relative a istruzione, formazione, didattica e orientamento scolastico. Altre sezioni, su tematiche relative a ricerca e innovazione, scienze e saperi, rischi di dipendenza dalla rete, robotica educativa e informatica forense, intendono offrire approfondimenti che coronano una visione interdisciplinare orientata ad una prospettiva olistica del Sapere.

Luigi A. Macri
Direttore Editoriale



Il materiale inviato non si restituisce, anche se non pubblicato. I contenuti degli articoli non redazionali impegnano i soli autori. Ai sensi dell'art. 6 - L. n.663 del 22/04/1941 è vietata la riproduzione totale o parziale senza l'autorizzazione degli autori o senza citarne le fonti.

Tutti i diritti riservati
www.ictedmagazine.com © 2022

Editoriale.....	pag. 4
<ul style="list-style-type: none"> • Il Tempo nell'era digitale <i>di Luigi A. Macrì</i> 	
Generazioni a confronto.....	pag. 5
<ul style="list-style-type: none"> • Sfruttamento sessuale on line dei minori <i>di Claudia Ambrosio</i> 	
Dalle Scuole	pag. 8
<ul style="list-style-type: none"> • La strada di casa: la tecnologia al servizio dei processi educativi <i>Classe terza SSAS IISS di Diamante</i> • Storytelling e competenze di cittadinanza digitale: una finestra aperta tra passato e presente <i>di Pasqualina Pace</i> 	
Didattica e Tecnologie	pag. 12
<ul style="list-style-type: none"> • L'intelligenza artificiale nella scuola di base: uno studio dell'Università della Finlandia Orientale. <i>di Mario Catalano</i> • Educazione aperta.... una questione di giustizia sociale <i>di Rosa Suppa</i> 	
Diritto e Informatica Forense	pag. 17
<ul style="list-style-type: none"> • Un nuovo modello di design organizzativo per la gestione della crisi energetica e il rapporto fra nuove tecnologie e innovazioni legislative <i>di Ludovica Zoccali</i> 	
Lavoro e Sicurezza.....	pag. 20
<ul style="list-style-type: none"> • Robotica collaborativa <i>di Paolo Preianò</i> 	
Robotica e pensiero computazionale.....	pag. 23
<ul style="list-style-type: none"> • Pensiero computazionale: imparare a sviluppare strategie fin da bambino <i>di Davide Sorrentino</i> 	
Sicurezza Informatica.....	pag. 25
<ul style="list-style-type: none"> • LOG4SHELL <i>di Benedetto Fucà</i> • Lo spear phishing e l'utilizzo di nuove tecniche con la social engineering <i>di Andrea Cortese</i> 	
ICT News.....	pag. 30
<ul style="list-style-type: none"> • Giornalisti in crisi, non la domanda di informazione <i>di Massimiliano Nespola</i> 	

IL TEMPO NELL'ERA DIGITALE

di Luigi A. Macrì

direzione@ictedmagazine.com



L'inizio di un nuovo anno scandisce, nelle nostre vite, uno dei momenti più carichi di aspettative e di riflessioni. Contiamo le ore, i minuti e poi perfino i secondi in attesa della mezzanotte, l'ora zero che dà inizio al nuovo anno. Poi durante le nostre giornate continuiamo a trattare il signor

Tempo, sì perché il Tempo è il nostro signore, come se non contasse nulla, come se fosse a nostra disposizione per riempirlo di piacevoli passatempi, di televisioni, di attività nelle reti sociali on line ed altro. Altre volte quando non siamo proprio convinti di qualcosa che ci chiedono di fare, o che abbiamo la possibilità di fare, diciamo a noi stessi: "Non ho tempo! Magari lo farò più tardi o un'altra volta!".

Una delle cose che, in questo contesto storico che stiamo vivendo, dovremmo dire a noi, stessi e che "è tempo di avere tempo", di abitare il tempo che velocemente scorre, farne lo spazio della nostra vita, rifuggendo pigrizie e inerzie che ci portano a procrastinare cose importanti che vogliamo realizzare nei nostri progetti.

Enzo Bianchi, saggista e monaco laico, fondatore della comunità monastica di Bose in Piemonte, in questi giorni, dalle pagine del Corriere della Sera, ci induce a riflettere su questi concetti e sul fatto che "questa disciplina del tempo è la condizione per pensare prima di fare, o meglio: per poter ritornare a pensare in questo inizio del millennio contrassegnato dall'esilio del pensiero proprio quando si dichiara di voler essere in connessione con il mondo intero".

Questa riflessione è ancora più importante in questo contesto storico nel quale il digitale assorbe troppo noi tutti, gli adolescenti e, purtroppo, anche i bambini e il mondo dell'infanzia.

Siamo strumenti di guadagno dei potentati mondiali delle tecnologie poiché tra motori di ricerca, pubblicità, notifiche e coinvolgimenti apparentemente gratuiti stiamo dando loro il NOSTRO TEMPO che di fatto diventa il LORO GUADAGNO. Oggi siamo nell'era del linguaggio iconico delle immagini, dei selfie, dei ritocchi sulle foto che si postano on line. Oggi la riflessione e gli approfondimenti su temi importanti per la nostra vita vengono il più delle volte percepiti con fastidio in

quanto significa impegno e lavoro, significa andare oltre la superficie delle cose e delle persone.

Se non riprendiamo la centralità del pensiero non possiamo rimodulare la necessaria centralità dell'Uomo e dell'Umanità.

Stiamo assistendo negli ultimi decenni ad un vero processo involutivo nel quale adolescenti e preadolescenti, unitamente a molti analfabeti di ritorno, basta vedere le statistiche dei libri che leggono i laureati, sono, loro malgrado, vittime e protagonisti di un vero e proprio processo involutivo; la capacità di parlare ed esprimere un pensiero articolato, approfondire tematiche analizzandone nella quotidianità i diversi aspetti sono competenze sempre meno diffuse.

Le tecnologie digitali, Internet e lo sviluppo della comunicazione e dell'informazione hanno, negli ultimi cinquanta anni, stravolto il mondo portando anche molti benefici ma la forza e gli interessi economici di chi ha guadagnato miliardi di dollari con le tecnologie e la pubblicità ci sta rendendo tutti strumenti in balia dei social, delle false notizie e, in breve, dell'ignoranza.

La ridondanza delle informazioni, la società dell'informazione sta diventando la società dell'informazione e dell'ignoranza. È stato provato dai ricercatori del M.I.T. - Massachusetts Institute of Technology, che le false notizie sono sei volte più veloci delle notizie vere. Quanto sta avvenendo in questo periodo di pandemia è sotto gli occhi di noi tutti. La soluzione la si può ricercare nella centralità del pensiero e dell'approfondimento ponendo l'Uomo e suoi valori al centro dello sviluppo delle tecnologie. Noi lavoriamo per una Tecnologia Umana, per catalizzare un futuro più umano: "Stiamo costruendo le piramidi della tecnologia umana. Immaginiamo un futuro in cui abbiamo una tecnologia non intrusiva che ci sta potenziando e che consente agli umani di fiorire e all'umanità di prosperare. Dove il mondo digitale è una naturale estensione di quello reale e un riflesso di noi stessi. Promuoviamo soluzioni che migliorano il benessere, la libertà e la società."



Sfruttamento sessuale on line dei minori

di Claudia Ambrosio

Abstract: *Le recenti misure di confinamento hanno portato ad un aumento del tempo trascorso su internet da parte dei minori, spesso senza supervisione e questo li ha resi più esposti alle pratiche di sfruttamento. Gli autori di abusi sessuali hanno approfittato della situazione pandemica per adescare le potenziali vittime tra i minori con un preoccupante aumento dei reati legati allo sfruttamento sessuale on line.*
* *Avvocato e Criminologa*

Spesso si corre il rischio di credere che quando i ragazzi sono al chiuso delle loro stanze, magari davanti al PC, siano al sicuro, lontani da pericoli per loro, ma questo è un falso mito poiché mai come oggi, soprattutto quando si passa molto tempo on line occorre un'attenta vigilanza poiché le maggiori insidie si hanno quando i minori finiscono vittima del più efferato cyber crime partendo da fenomeni come l'adescamento di questi (grooming) ai fini del loro sfruttamento pedopornografico (attraverso il file sharing), sessuale (anche tecnomediatore, il c.d. sexting), o, da ultimo, anche in termini di spettacoli o pubblicazioni oscene.

Sul punto, durante la pandemia, si registra un preoccupante peggioramento: anno dopo anno, in occasione della Giornata Nazionale contro la Pedofilia e la Pedopornografia, i dati sull'abuso e lo sfruttamento sessuale dei minori appaiono in costante crescita, con un ruolo degli abusi online sempre più marcato; a livello mondiale si è passati da 1 milione di segnalazioni nel 2010 a quasi 17 milioni nel 2019, con quasi 70 milioni di immagini e video.

Save the Children Italia realizza fin dal 2001 un servizio che consente agli utenti di Internet di segnalare la presenza di presunto materiale pedopornografico online tramite la piattaforma dedicata, nel 2020 le segnalazioni sono aumentate di circa il 30% rispetto al 2019 con l'effetto che dalle segnalazioni emerge che l'UE accoglie il maggior numero di materiale pedopornografico su scala mondiale.

Il legislatore nazionale, sulla scia di quanto emerso a livello internazionale, ha dovuto dar luogo ad una vera e propria evoluzione normativa sui reati implementando progressivamente il corpo del codice penale a partire dalla L. n. 269/98 *Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno dei minori* e a seguire poi con la L. n. 38 del 2006 *“Disposizioni in materia di lotta contro lo sfruttamento sessuale dei minori e la pedopornografia anche a mezzo internet”* con la quale si è operato un successivo intervento normativo diretto ad affinare la disciplina già delineata

sia attraverso l'introduzione di alcune modifiche alle disposizioni già formulate dalla precedente legge del 1998, sia ancora attraverso l'introduzione di nuove fattispecie quali la pedopornografia “virtuale”.

Le varie categorie dei fenomeni rientranti nella pedofilia online si rifanno a due principali filoni: quello relativo ai contenuti delle immagini e quello relativo ai contatti intercorsi tra vittima ed abusante, i dati mostrano anche un aumento dei casi di estorsioni a sfondo sessuale e di cyber-grooming, inoltre le tecnologie digitali da un lato hanno facilitato il compito ai criminali, permettendo loro di raggiungere più facilmente i minori tramite l'uso di webcam, dispositivi connessi e chat room sui social media e nei videogiochi; dall'altro ne hanno garantito l'anonimato grazie all'uso di tecnologie come il cloud computing e il dark web.

Nel corso degli anni, si sono verificati numerosi casi di “adescamento di minorenni”, soprattutto a causa dell'avanzamento del sempre più insidioso mondo digitale, il quale agevola non solo la commissione di tale fattispecie di reato, ma di molteplici altri illeciti penali: il legislatore affronta compiutamente la problematica in primis con l'articolo 609 undecies del Codice Penale che disciplina il reato di “adescamento di minorenni”, si tratta di un reato comune conosciuto anche come “child grooming”.

L'articolo in esame è stato aggiunto dall'art. 4 comma 1, lett. z) della Legge 172/2012 (Legge di Ratifica della Convenzione di Lanzarote per la protezione dei minori contro lo sfruttamento e l'abuso sessuale), le c.d. “condotte child grooming” sono diffuse soprattutto nei paesi informatizzati e vengono realizzate mediante tecniche di manipolazione psicologica atte ad indebolire le volontà della vittima e creare un rapporto di confidenza con l'adescatore per fini di sfruttamento o abuso, il bene giuridico che la norma intende tutelare è la libertà sessuale e di autodeterminazione, anche nello sviluppo sessuale del minore, in relazione alla sua sensibilità, maturazione



ed evoluzione psichica e sessuale.

L'art. 609 undecies prende in considerazione e tutela, come soggetto passivo del reato, il minore di anni 16, trattandosi di un reato comune, il soggetto attivo può essere chiunque, solitamente, si tratta di soggetti adulti, di età notevolmente superiore rispetto al minore adescato, affinché il reato possa considerarsi integrato, non è necessaria la consumazione, essendo sufficiente che vengano poste in essere condotte meramente preparatorie, si tratta, dunque, di un reato di pericolo volto a neutralizzare il rischio.

In particolare, la norma punisce con la reclusione da uno a tre anni, se il fatto non costituisce più grave reato, chiunque adesci un minore di anni 16, allo scopo di commettere i reati di cui agli articoli 600, 600 bis, 600 ter, 600 quater, anche se relativi al materiale pornografico di cui all'art. 600 quater. 1, 600 quinquies, 609 bis, 609 quater, 609 quinquies, e 609 octies; l'articolo 609 undecies specifica che con il termine "adescamento" si intende qualsiasi atto volto a carpire la fiducia del minore attraverso artifici, lusinghe o minacce, posti in essere anche mediante l'utilizzo della rete internet o di altre reti o mezzi di comunicazione.

Significativo sotto tale profilo la coincidenza con il concetto giuridico di adescamento con quello criminologico, posto che anche nella descrizione del profilo del reo di tale tipologia di condotta si tratteggia questo tipo di tratto comportamentale.

L'adescamento, infatti, ha inizio nel momento in cui l'adulto mostra particolare interesse nei confronti del minore per instaurare un solido legame di fiducia questa dinamica inizia con l'adulto che, mentendo sulla propria età, propone alle vittime conversazioni su temi di loro interesse (sport, giochi, scuola); l'adulto presta attenzione ai racconti, è premuroso e si dichiara suo grande amico: il processo di manipolazione per ottenere la totale fiducia del minore può durare diverso tempo in

una vera e propria escalation criminale.

Gradatamente l'adulto ricerca un contatto sempre più intimo e privato fino alla manifestazione dell'abuso e per ottenere il silenzio si arriva al ricatto di mostrare le immagini o il contenuto delle conversazioni a genitori, amici, o diffonderle su internet.

La Corte di Cassazione ha sottolineato come "le condotte artificiali, lusinghiere o minacciose, volte a carpire la fiducia del minore, seppur moralmente discutibili, sono considerate lecite dal punto di vista giuridico perché idonee a costituire un pericolo concreto per il corretto sviluppo psico-fisico e la libera autodeterminazione del soggetto adescato.

Le stesse perdono il requisito della liceità e diventano sanzionabili a titolo di adescamento, quando risultino finalizzate al compimento di reati di sfruttamento o abuso a danno del soggetto vulnerabile, perché solo in quel caso acquisiscono quel livello di pericolosità idoneo a costituire un rischio concreto per la persona offesa".

Recentemente, la Suprema Corte di Cassazione ha puntualizzato che l'art. 609 undecies punisce le condotte di "victim selection", attraverso le quali l'agente, spinto dal movente sessuale, dopo aver selezionato la vittima e preso contatti con essa, instaura un rapporto intimo e confidenziale ne carpisce la fiducia, introduce la tematica sessuale e le rivolge i primi inviti.

Successivamente, si passa al c.d. "sexual stage", ricompreso nell'ambito del tentativo: in questa fase, sottolinea la Cassazione, l'agente inizia ad esercitare pressioni nei confronti del minore vittima, al fine di organizzare un vero e proprio incontro.

La condotta appena descritta (sexual stage) come già detto, rientra nell'ambito del tentativo, in quanto "cronologicamente più vicina alla consumazione del reato a sfondo sessuale", ed essendo considerata più rischiosa per l'effettiva lesione del bene giuridico tutelato, viene punita con una sanzione più severa.

Con specifico riferimento ai casi di adescamento "online", è possibile trovarsi di fronte a situazioni in cui un soggetto non sia a conoscenza della reale età della "vittima", la quale può facilmente mentire riguardo i propri dati anagrafici, facendo credere il falso a chi si trovi dall'altra parte dello schermo, pertanto, l'art. 609 sexies, con riferimento ai reati in materia sessuale, sancisce che "quando i delitti previsti negli artt. 609 bis, 609 ter, 609 quater, 609 octies e 609 undecies sono commessi in danno di un minore degli anni 18, e quando è commesso il delitto di cui all'art. 609 quinquies, il colpevole non può invocare

a propria scusa l'ignoranza dell'età della persona offesa, salvo che si tratti di ignoranza inevitabile".

Sul fronte della vittima, queste azioni comportano umiliazione, lesione della propria immagine e della propria dignità, condizionamenti nei rapporti sociali, forti disagi all'integrità psichica.

A luglio il Parlamento europeo ha approvato alcune norme temporanee per consentire ai fornitori di servizi di posta elettronica, chat e messaggistica online di individuare, rimuovere e segnalare volontariamente i casi di abusi sessuali su minori, nonché di permettere l'utilizzo di tecnologie a scansione per contrastare i tentativi di abuso dei minori.

Le nuove tecnologie permettono, infatti, di aiutare a rilevare materiale contenente abusi sessuali sui minori: attraverso l'hashing per esempio è possibile scansionare contenuti come immagini e video, mentre attraverso l'intelligenza artificiale è possibile analizzare testi o dati di traffico online, in modo da rilevare alcune pratiche di adescamento presenti in rete.

Quella dello scambio di immagini illegali tra utenti della rete è la dimensione più significativa del fenomeno della pedofilia on-line, lo scambio di materiale avviene attraverso l'uso di qualsiasi spazio o servizio web dapprima le chat tematiche, poi i vari circuiti di file sharing, i forum, i socialnetwork, ecc.

La commercializzazione rappresenta la dimensione organizzata, il business che proviene dalla produzione e dalla vendita di pedopornografia in siti a pagamento: l'attuale nuova tendenza è quella che sfrutta i servizi del web per la prostituzione di minori, ovvero per la perpetrazione di abusi dietro pagamento da parte di committenti che fruiscono della visione di tali comportamenti delittuosi.

Con la Ratifica della Convenzione di Lanzarote, avvenuta attraverso la promulgazione della Legge n.172/2012, questa tipologia di siti può ricondursi alle previsioni di apologia ed istigazione delle pratiche in argomento

contemplate nell'art 414 bis c.p.

La fattispecie punisce con la reclusione da un anno e sei mesi a cinque anni, e salvo che il fatto costituisca più grave reato, chiunque, con qualsiasi mezzo e con qualsiasi forma di espressione, pubblicamente istiga a commettere o fa apologia di uno o più dei seguenti delitti in danno di minori:

- prostituzione minorile (art. 600-bis);
- pornografia minorile e detenzione di materia pedopornografica anche in riferimento a immagini virtuali (artt. 600-ter, 600-quater, 600-quater.1);
- turismo sessuale (art. 600-quinquies);
- violenza sessuale semplice e di gruppo in danno di minorenni (artt. 609-bis e 609-octies);
- atti sessuali con minorenni (art. 609-quater);
- corruzione di minorenni (art. 609-quinquies).

Fin qui il copioso quadro normativo dal quale si evince una peculiare attenzione del legislatore sulla materia in esame, tuttavia, anche in tale settore la tutela solo normativa, per quanto imprescindibile, da sola non è soddisfacente.

Le leggi attuali di contrasto alla criminalità informatica, infatti, non sono sufficienti: a causa della difficoltà che hanno le vittime di cyber-crime a far valere i loro diritti, il tempo per ottenere l'oscuramento di un sito è troppo lungo e avviene solo a livello nazionale e non mondiale, con evidenti limiti nella tutela di chi è colpito da queste forme di persecuzioni, non si dimentichi, poi che quando la norma interviene il "danno" è già fatto con conseguenze spesso devastanti soprattutto per le giovani vittime; ad oggi, pertanto, ancora una volta è la sinergia tra prevenzione e legislazione ad apparire come lo strumento preferibile al fine del contenimento degli abusi anche on line dei minori.



La strada di casa: tecnologie e processi educativi e formativi a cura di Rosa Suppa*

Abstract - "Hai presente quelle situazioni...quelle situazioni della vita in cui sei stato travolto da un vortice emozionale che ti ha paralizzato e non riesci più a concentrarti sulle cose...hai l'impressione di uscire da te stesso... è come perdersi in un deserto senza riuscire più a trovare la strada... la strada di casa".

* Docente di Filosofia - Gruppi telelavoro studenti e studentesse le studentesse e gli studenti della classe terza S.S.A.S. I.I.S.S. di Diamante



“La strada di casa” è il titolo che le studentesse e gli studenti dell’Istituto di Istruzione superiore di Diamante, nell’ambito del corso di studio professionale per i servizi per la sanità e l’assistenza sociale, hanno scelto per una attività di ampio respiro, che li ha fatto lavorare all’interno di un setting laboratoriale educativo e didattico autonomamente gestito.

La tematica, declinata durante le lezioni di psicologia applicata, è emersa a seguito di momenti differenti di lavoro e condivisione: brainstorming, focus group, role playing.

Gli incontri hanno fatto emergere, in un contesto protetto pensieri ed emozioni particolarmente interessanti ed intensi.

Secondo la prospettiva riflessiva degli studenti e delle studentesse “Il bullo è forte solo perché non riesce ad ammettere le personali debolezze e il bullismo

rappresenta una forma di violenza sia fisica che psicologica che annienta le persone fragili perché determina isolamento, non fiducia nell’altro, paura, senso di inefficacia, perdita dell’autostima, umiliazione e tristezza.

«Il bullizzato dall’altra parte è una persona umana che “scoppia dentro” anche per una piccola futilità, la personalità di questo soggetto si sgretola gradatamente ma drammaticamente e pian piano non riuscirà più a riconoscersi.

Il cyberbullismo, quale prosieguo di una situazione di vessazione sistematica, presenta tuttavia una connotazione maggiormente subdola perché implica il “nascondimento” dietro uno schermo”, questi appunto, attraverso lo scudo dello schermo si protegge dall’incapacità di relazionarsi alla pari con l’altro da sé.

È necessario attribuire alle parole il giusto peso e agire attivamente nei contesti educativi, formativi e di istruzione per «fermare le violenze».

Le tematiche del bullismo e del cyberbullismo, hanno rappresentato pertanto il file rouge dei vari momenti di immersione educativa, che hanno lasciato spazi a tutte/i e a ciascuna/o, nell'ottica di un libero pensiero



che si interroga e poi guida l'azione consapevolmente. Gli studenti e le studentesse hanno deciso di effettuare una rielaborazione delle riflessioni maturate creando due gruppi di lavoro e pianificando due prodotti coerentemente con le finalità del loro percorso di studi: un video educativo di monito al bullismo e al cyberbullismo e un fumetto.

I gruppi di lavoro hanno cominciato a confrontarsi, organizzando le due attività, ne è conseguita una suddivisione dei compiti, la redazione di un progetto e dunque la stesura di una story board per ciascun prodotto e la selezione delle comparse o attori.

I personali device hanno integrato la dotazione informatica della scuola e così sono cominciate le riprese, poi è seguita la fase della scelta della musiche, il montaggio e dunque la cernita delle scene per la messa in opera del prodotto.

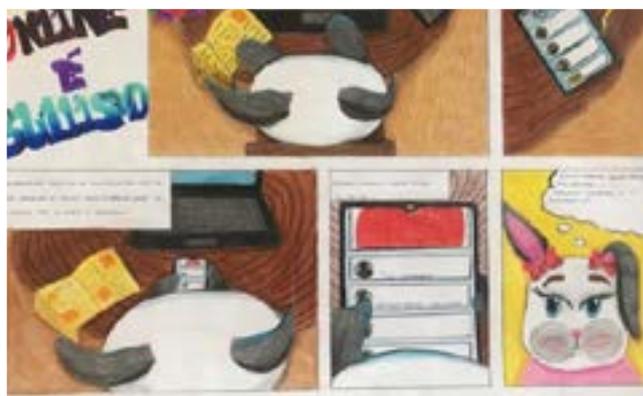
Non sono mancati piccoli problemi nei quali tuttavia il gruppo classe ha dimostrato un forte spirito di coesione e adattamento.

L'Istituzione scolastica di Diamante si muove come tutte le altre istituzioni scolastiche nazionali, nella dimensione delle competenze trasversali e competenze chiave dove i percorsi disciplinari specifici ben coniugati con i vari saperi sollecitano le menti al fine di far maturare competenze di imprenditoria, cittadinanza attiva e consapevole

Il video si rivolge all'utenza più vasta e se anche parte da premesse negative, nella parte conclusiva, comunica un messaggio di condivisione e amicizia.

Il fumetto e-book vuole rivolgersi ai bambini ed è orientato ad un percorso di sensibilizzazione al

tema del bullismo dei più piccoli, attraverso il potente strumento della narrazione, che vede protagonisti alcuni coniglietti, si riflette sulle emozioni e sui comportamenti pericolosi.



Ritrovare “La strada di CASA” è possibile mediante l'uso consapevole della tecnologia che diventa strumento potentissimo al servizio dell'educazione e della formazione.

I lavori sono visionabili sul sito della scuola all'indirizzo <https://www.iissdiamante.edu.it/>

Le studentesse e gli studenti della classe terza S.S.A.S.

I.I.S.S. di Diamante

Isabella Arieta, Giulia Campagna, De Brasi Naomi, Ylenia Fortunato, Martina Guglielmi, Francesco La Badessa, Angelo Laino, Angelo Carmelo Liserre, Candida Maria Raffaele, Francesco Magurno, Nizar Razaq, Valentito Toto, Anastasia Valdevit, Angel Zhan.

Coordinamento attività Prof.ssa Rosa Suppa

Storytelling e competenze di cittadinanza digitale: una finestra aperta tra passato e presente

di Pasqualina Pace*



Abstract - In epoca pandemica, non è facile creare ambienti educativi collaborativi, ma il “non facile” non corrisponde all’impossibile. Reinventarsi per “imparare insieme”, è stata la sfida che ci siamo lanciati. Siamo in una classe V di Scuola Primaria nell’anno 2020, che si apre con una grande novità: la DDI per gli alunni fragili. Come creare allora un ponte educativo, emotivo e collaborativo tra i due ambienti educativi, quello in presenza e quello a distanza? Bene, buttiamoci nella mischia e partecipiamo al Premio Scuola Digitale con un prodotto multimediale che ci ha offerto la possibilità di lavorare insieme anche se a distanza, attivando competenze digitali e sociali di Cittadinanza Digitale attraverso il Digital Storytelling. La scelta ricade sull’utilizzo dell’app Book Creator, uno strumento per la creazione di libri digitali intuitivo, completo che ha

permesso ad ogni bambino di confrontarsi, pianificare e prendere decisioni creative sul contenuto del libro.

* docente di Scuola Primaria, componente del Team Digitale, Staff di direzione, Comitato di Valutazione, Referente di Plesso IC Pescara 10. Dirigente Scolastico Prof.ssa Stefania Petracca



La classe 5C del Plesso Carducci IC Pescara 10, all’interno della programmazione curriculare, ha portato avanti il Project Work di Digital Storytelling partendo dalla celebrazione della giornata della memoria.

“Ricordare per non dimenticare”, è un mantra che risuona nelle nostre vite, ma ricordare cosa, non dimenticare chi! La necessità di avviare un percorso di didattica della memoria appare quanto mai utile e necessaria se guardiamo la realtà che ci è intorno e non è mai stata intesa, nel mio fare scuola, come un’esperienza isolata nel percorso scolastico, delegata solo al 27 gennaio. Perché

ricordare il virologo di origini ebraiche Albert Sabin? Perché in tempi di feroci dibattiti e contrapposizioni sui vaccini anti-Covid, regalare ai lettori la sua storia, raccontarla e metterla a disposizione di tutti attraverso il web, possa far comprendere la valenza scientifica di una

vaccinazione massiva. Il nostro ebook racconta la storia del dottor Albert Sabin, il medico polacco che restituì l’estate ai bambini grazie alla scoperta del vaccino contro la poliomielite. Ebreo di origine, durante le persecuzioni antisemite, visse la perdita di



due nipotine uccise in un campo di concentramento nazista, ma **Albert Bruce Sabin** si vendicò a modo suo, inventando il vaccino contro la poliomielite, non brevettandolo ma rendendolo disponibile gratuitamente a tutto il mondo. Quando gli chiesero perché aveva fatto una cosa del genere, lui rispose: *“Le SS mi hanno ucciso due meravigliose nipotine, ma io ho salvato i bambini di tutta l’Europa. Non la trovate una splendida vendetta?”*. Il vaccino contro la poliomielite elaborato dal dottor Albert Sabin, che falliva una volta su 750 mila somministrazioni, ha salvato negli anni milioni di vite. E adesso? Sarà possibile avere un nuovo Sabin? Questa la domanda a cui il mondo deve rispondere ai nostri bambini.

La sfida condivisa di questo gruppo di 24 bambini, di cui 2 in DDI ha inizio.

Siamo a metà gennaio del 2020.

Tutta l’attività, proposta con contenuti multidisciplinari, è stata ripensata e pianificata secondo una visione più organica, che superi la dimensione strettamente disciplinare, per permettere l’attiva e significativa partecipazione di tutti gli alunni nel rispetto delle reali potenzialità e dei bisogni di ciascuno, nessuno escluso.

L’utilizzo di una metodologia didattica non tradizionale, attraverso l’utilizzo dei New Media per lo sviluppo delle Life Skills e delle competenze digitali, ha avuto lo scopo di trasformare una difficoltà creata da una frequenza scolastica a due velocità, (un gruppo in classe e uno che segue da casa), in una opportunità. La metamorfosi che al tempo del Covid-19 poteva trasformarsi per i ragazzi in un’onda anomala, è diventata una certezza: occorre attrezzarsi per fronteggiare la lontananza dalla classe e la solitudine nelle proprie case: tutti i bambini, sia quelli in presenza che quelli inseriti in DDI, si sono sentiti parte di un unico gruppo che ha lavorato per uno

scopo comune. Abbiamo dato vita ad un terzo spazio, ad un terzo tempo più **partecipati e collaborativi**, nei quali il coinvolgimento diretto e attivo dello studente ha facilitato la personale co-costruzione dei saperi, **potenziando l’apprendimento degli studenti** in tutte le sue sfaccettature- ossia a **livello formale, non formale e informale**.

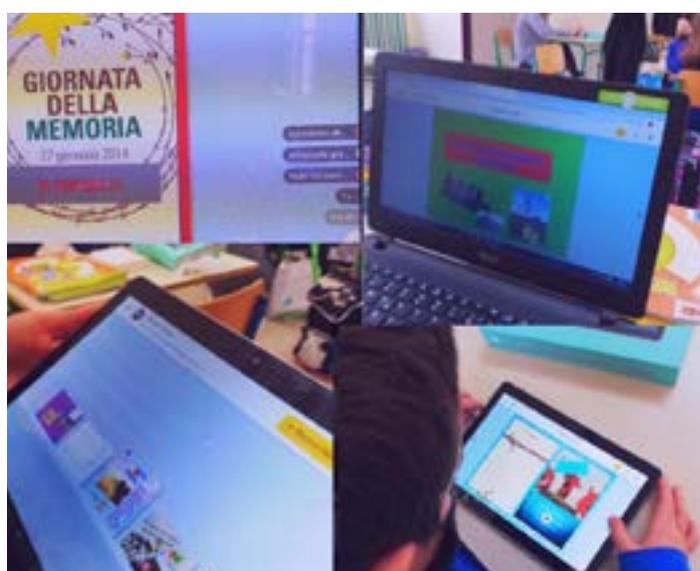
Gli alunni divisi in gruppi cooperativi hanno prodotto CDD (Contenuti Didattici Digitali) con Google Heart, Spick pic, Voki, Time line, Powtoon, Youtube, Classroom per l’implementazione del libro digitale realizzato con l’app Book Creator, con la pratica del BYOD/BYOT (Bring Your Own Tecnology/Device), consolidando e potenziando il proprio bagaglio di conoscenze. Durante il percorso si è favorito l’apprendimento cooperativo e si sono rafforzati il senso di fiducia e di rispetto

Il digitale è stato il mezzo/strumento per la creazione della risorsa digitale, che è risultata secondaria rispetto a tutto il processo di apprendimento- insegnamento.

La chiusura della scuola per il contenimento della pandemia, a marzo, non ci ha fermati, abbiamo continuato a lavorare in maniera collaborativa, dando la possibilità ai giovani studenti di scoprire la gratificante sensazione che si prova quando il frutto della loro creatività prende realmente forma e si realizza grazie al contributo di ognuno di loro.

E la sfida continua: partecipiamo al Premio Scuola Digitale. Lo spirito di collaborazione, il senso di appartenenza ad un gruppo di lavoro, ci ha permesso di ottenere il I° posto alla provinciale e II posto alle regionali Abruzzo (perso il I posto per 0,4 punti).

Per leggere il nostro lavoro clicca sul [link](#)



L'intelligenza artificiale nella scuola di base: uno studio dell'Università della Finlandia Orientale.

di Mario Catalano*



Abstract: è fondamentale che gli studenti di oggi, sin dagli anni della scuola di base, comprendano la logica e il ruolo sociale dei modelli di intelligenza artificiale, che stanno rapidamente trasformando il mondo in cui viviamo e prefigurando grandi opportunità per il futuro, esigendo, tuttavia, una grande attenzione alle possibili ricadute negative in ambito etico. Questo articolo intende dare un contributo in tale direzione, illustrando le linee essenziali di una recente ricerca pubblicata dalla rivista scientifica "International Journal of Child-Computer Interaction" e realizzata da un team multidisciplinare di studiosi dell'Università della Finlandia Orientale. Questi ricercatori hanno voluto esplorare, tramite analisi qualitative, le potenzialità di contesti di apprendimento in cui studenti di 12 e 13 anni siano chiamati ad immaginare problemi della vita quotidiana da risolvere con applicazioni di intelligenza artificiale, nonché progettare e realizzare i relativi modelli di machine learning con la guida dei docenti e di esperti di computer science.

*Ricercatore, Docente, Editore Scientifico.

Questo articolo illustra le linee essenziali di una recente ricerca (Fig. 1) pubblicata dalla rivista scientifica "International Journal of Child-Computer Interaction" (Vartiainen et al., 2021) e realizzata da un team multidisciplinare di studiosi dell'Università della Finlandia Orientale (School of Applied Educational Science and Teacher Education; School of Computing). Essi hanno esplorato l'apprendimento del machine learning attraverso esperienze laboratoriali nella scuola media. In particolare, i ricercatori hanno voluto comprendere, tramite analisi qualitative, le potenzialità di contesti di apprendimento in cui studenti di 12 e 13 anni siano chiamati ad immaginare problemi della vita quotidiana da risolvere con applicazioni di intelligenza artificiale, nonché progettare e realizzare i relativi modelli di machine learning con la guida dei docenti e di esperti di computer science.

Nella visione di questi ricercatori, tutto ciò risponderebbe alla crescente esigenza di capire come le istituzioni educative possano preparare le giovani generazioni al ruolo di cittadini attivi, professionisti ed innovatori della società digitale (Hints et al., 2019;

Shapiro et al., 2018). Inoltre, convinti dell'efficacia di quelle esperienze di formazione in cui gli allievi si servano creativamente delle tecnologie per affrontare problemi significativi (Brennan and Resnick, 2012; Papert, 1980; Papert and Harel, 1991; Resnick, 2017), hanno concentrato l'attenzione su due fondamentali domande di ricerca:

- 1) gli studenti della scuola media sarebbero capaci di immaginare e progettare modelli ed applicazioni di machine learning per il soddisfacimento di bisogni della vita quotidiana, da loro stessi considerati rilevanti?
- 2) In che modo la progettazione e realizzazione di tali modelli ed applicazioni, con la guida di esperti di computer science, può influire sulla comprensione della logica, delle potenzialità e dei rischi del machine learning?

In particolare, il progetto di ricerca ha coinvolto 34 alunni di 12-13 anni di una scuola di base finlandese, proponendo loro tre workshop di 2-3 ore ciascuno e delle interviste strutturate, e ha previsto, altresì, osservazioni sistematiche condotte dai ricercatori lungo tutto il percorso.

All'inizio, gli studenti sono stati invitati ad esprimere con linguaggio verbale ed iconico le loro conoscenze sul modo di operare degli algoritmi di machine learning (ad esempio, con tale tipologia di quesiti: come sarebbe possibile insegnare ad una macchina a distinguere l'immagine di un fiore da quella di un gatto?). Anche alla fine dell'esperienza, gli allievi si sono misurati con un simile compito, in modo



Fig. 1 Immagine tratta dalla pubblicazione descritta in questo articolo

da poter valutare qualitativamente i loro progressi nella conoscenza della logica e del potenziale ruolo sociale dell'intelligenza artificiale.

Il primo workshop ha introdotto i ragazzi nel mondo dell'apprendimento delle macchine attraverso la spiegazione da parte di insegnanti esperti dei concetti di base e l'esame di casi reali. Inoltre, gli studenti hanno potuto familiarizzare con la piattaforma Google Teachable Machine, che è una delle più popolari applicazioni web per lo sviluppo di modelli di intelligenza artificiale indirizzata a chi non abbia conoscenze e competenze avanzate nel campo della matematica e della programmazione. Permette, pertanto, anche ai più giovani ed inesperti, di addestrare e valutare modelli di machine learning per la classificazione di immagini, gesti, suoni. Così, gli alunni hanno potuto esplorare la fase di addestramento, in cui si scelgono gli esempi da cui la macchina deve imparare a classificare un oggetto reale (Fig. 2), e quella di valutazione dell'accuratezza, in cui la macchina addestrata è chiamata a classificare un nuovo caso (mai incontrato!) esplicitando, attraverso un valore di probabilità, il suo livello di "fiducia" (confidence) nella previsione generata (Fig. 3). Alla fine di questo primo workshop, agli allievi è stato chiesto di individuare alcuni bisogni della vita quotidiana che potrebbero essere soddisfatti con applicazioni web basate su algoritmi di intelligenza artificiale.

Nel secondo workshop, dopo aver selezionato nove idee progettuali, i ricercatori hanno suddiviso i partecipanti in altrettanti team di lavoro, stimolandoli a descrivere più in dettaglio le applicazioni proposte: funzioni essenziali, tipologia e fonti dei dati richiesti per l'addestramento del modello di classificazione (immagini, suoni, etc.), categorie che il modello dovrebbe riconoscere, ... Inoltre, in questa fase, gli studenti hanno immaginato e rappresentato

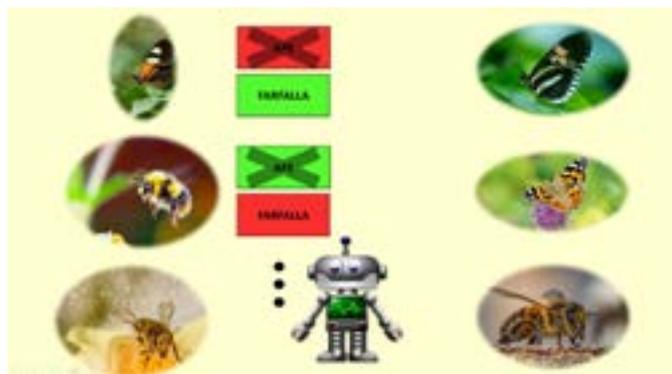


Fig. 2 Esempio di addestramento di un modello di machine learning per la classificazione delle immagini

graficamente l'interfaccia dell'applicazione prescelta e, con il supporto degli esperti coach, hanno addestrato, valutato e iterativamente affinato i relativi modelli servendosi della Google Teachable Machine.

Infine, nel terzo workshop, gli allievi hanno avuto la possibilità di confrontarsi con gli esperti sull'intero processo, nonché collegarsi alle applicazioni web sviluppate dai soli ricercatori (sulla base dei loro progetti e dei modelli di classificazione creati insieme), sperimentarne le funzioni, l'accuratezza e i limiti, in modo da poterle illustrare ai loro pari e ai docenti.

L'analisi delle osservazioni effettuate lungo tutto il percorso e del feedback degli studenti intervistati ha rivelato che gli allievi, non avendo inizialmente (per lo più) alcuna idea chiara dei principi sottesi ai processi di machine learning, sono riusciti a maturare la capacità empatica di riconoscere ed analizzare bisogni collettivi rilevanti legati alla vita quotidiana e a quella scolastica, nonché una comprensione soddisfacente della logica induttiva che caratterizza il modo in cui le macchine "imparano", dagli esempi, a svolgere compiti di classificazione troppo complessi per essere codificati con la tradizionale programmazione digitale (approccio rule-based).

Più in particolare, è stata molto preziosa l'esperienza con i dati, che ha fatto capire ai giovani partecipanti come eventuali asimmetrie (pochi esempi o esempi poco diversificati per una certa categoria) possano influire molto negativamente sulla precisione delle classificazioni.

Sorprendente, poi, la creatività mostrata dai ragazzi nel concepire applicazioni di intelligenza artificiale che risolvessero problemi concreti: riconoscimento di gesti per attivare l'apertura e la chiusura di porte automatiche, riconoscimento di suoni ed immagini per il funzionamento di distributori automatici di cibo per gatti, correttori digitali di compiti scolastici tramite la decodificazione di testi scritti a mano, classificatori della tossicità potenziale di funghi e bacche attraverso abilità di computer vision, detector in grado rilevare gli studenti che disturbano durante l'assenza temporanea di un insegnante dall'aula, riconoscimento facciale per l'identificazione dei criminali a supporto delle operazioni di polizia, etc.

In alcuni casi, è emersa anche la consapevolezza da parte degli alunni del possibile impatto dell'automazione dei servizi sul mercato del lavoro: ad esempio, una studentessa, interessata a sistemi automatici di pagamento negli esercizi commerciali, si è espressa

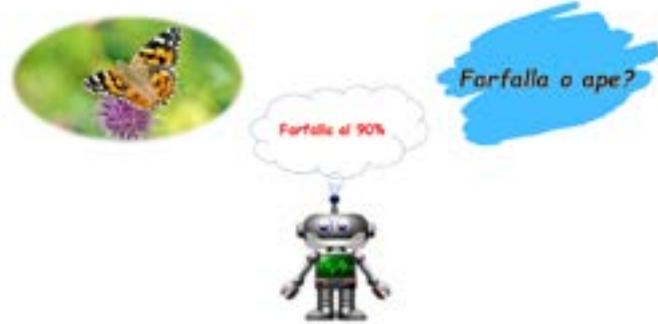


Fig. 3 Esempio di test di un modello di machine learning per la classificazione di immagini.png

<http://www.papert.org/articles/SituatingConstructionism.html>.
 Resnick, M. (2017). *Lifelong kindergarten: Cultivate creativity through projects, passion, peers, and play*. Cambridge, MA: MIT Press.
 Shapiro, B., Fiebrink, R., and Norvig, P. (2018). *How machine learning impacts the undergraduate computing curriculum*. *Communications of the ACM*, 61(11), pp. 27–29.
 Vartiainen, H., Toivonen, T., Jormanainen, I., Kahila, J., Tedre, M., and Valtonen, T. (2021). *Machine learning for middle schoolers: Learning through data-driven design*. *International Journal of Child-Computer Interaction*, Volume 29.

circa la scomparsa della figura tradizionale del cassiere.

Gli autori dello studio hanno, tuttavia, manifestato delle perplessità sulla presentazione dei modelli di machine learning come delle black-box: infatti, strumenti come la Teachable Machine dissimulano la struttura fondamentale dei suddetti modelli su cui, probabilmente anche nella scuola di base, con un linguaggio semplice e con metodo analogico (magari avvalendosi del potere evocativo delle metafore), si potrebbe approfondire un po' di più; la comprensione delle reti neurali artificiali, ad esempio, potrebbe giovare particolarmente di tali approcci. Inoltre, hanno ravvisato una seria lacuna nell'assenza di una dimensione etica del confronto tra gli studenti e gli esperti sul ruolo sociale dell'intelligenza artificiale. Il superamento di questi limiti e l'ampliamento del campione per diversificare il contesto e le caratteristiche socio-economiche dei partecipanti rappresentano le future direzioni di sviluppo di questa affascinante ricerca.

BIBLIOGRAFIA:

- Brennan, K., and Resnick, M. (2012). *Using artifact-based interviews to study the development of computational thinking in interactive media design*. Paper presented at annual American Educational Research Association meeting, Vancouver, BC, Canada.
- Hintz, A., Dencik, L., and Wahl-Jorgensen, K. (2019). *Digital citizenship in a datafied society*. Cambridge, UK: Polity Press.
- Papert, S. (1980). *Mindstorms: Children, Computers, and Powerful Ideas*. Basic Books, Inc., New York, NY, USA. Disponibile all'indirizzo: <http://dspace.mit.edu/handle/1721.1/5837>
- Papert, S., and Harel, I. (1991). *Situating constructionism*. In *Constructionism*.



Educazione Aperta... una questione di giustizia sociale

di Rosa Suppa*

Abstract - Giustizia sociale quale l'accesso a coloro che non potrebbero altrimenti accedere all'esperienza di apprendimento, ridisegnando l'esperienza di apprendimento [...] riconoscendo la cultura delle minoranze.

*Docente di Filosofia e Scienze umane

Le pratiche educative aperte, spesso indicate con la sigla O.E.P., riguardano attività che prevedono l'uso di risorse educative aperte nei processi di istruzione, tuttavia le pratiche educative aperte comprendono forme svariate di apertura addirittura senza l'impiego di risorse aperte (OER).

Il 15 settembre del 2007 a Città del Capo in Sudafrica è stata redatto una interessante documento, la DICHIARAZIONE SULL'ISTRUZIONE APERTA.

Nel testo si afferma che quando si parla di educazione aperta non bisogna intendere le sole O.E.R. perché in realtà essa "attinge anche a tecnologie aperte che facilitano l'apprendimento collaborativo e flessibile e la condivisione aperta delle pratiche didattiche"¹.

L'educazione aperta così intesa si coniuga perfettamente con un altro interessantissimo tema la Social Justice che apre ampi scenari anche in riferimento al concetto di sostenibilità e agli obiettivi che in esso trovano dimora.

«In ambito educativo la giustizia sociale è un tema costantemente presente [...] ancor più se ci si muove

nello scenario della Open Education e delle attività in corso per riuscire, entro il 2030, a raggiungere l'obiettivo di sostenibilità fissato dalle Nazioni Unite rispetto all'educazione, *Quality education for all* (SDG 4²)»³.

Nella prospettiva della sostenibilità infatti l'Open Education diventa approccio strategico atto a ridisegnare il mondo, secondo i principi di giustizia ed equità, e ad analizzare questioni salienti quali: digital divide, decolonizzazione dell'educazione, inclusione sociale, allargamento della partecipazione. La dottoressa Nancy Fraser, docente di filosofia politica ed etica normativa alla New School for Social Research di New York, ha teorizzato un interessante modello di giustizia sociale che focalizza l'attenzione «su tre temi strategici.

1. L'economia (nella tensione tra redistribuzione e maldistribuzione);
2. la cultura (per il rapporto tra riconoscimento e disconoscimento);



3. la politica (per la dinamica tra partecipazione ed esclusione): non c'è redistribuzione né riconoscimento, senza partecipazione».

«Si può considerare che l'OEP spazia su tre dimensioni generali, incluse alcune sotto-dimensioni, quali:

1. Da content-centric a process-centric;
2. Da incentrato sull'insegnante a incentrato sullo studente;
3. Da principalmente pedagogico a principalmente focalizzato sulla giustizia sociale. Se principalmente focalizzata sulla giustizia sociale, possiamo considerare il grado in cui si rivolge:
 1. Economico e/o
 2. Culturale e/o
 3. Ingiustizia politica».

Il primo asse, che va dal contenuto alla centralità del processo, prevede che lo scopo principale dell'OEP è quello di produrre o creare OER incentrati sul contenuto; ma se lo scopo principale è invece concentrarsi sui processi di interazione tra i partecipanti, allora è più incentrato sul processo».⁴

Si tratta di una dinamica di co-costruzione del sapere che attiva principi connettivisti «che mette in primo piano il valore delle diverse opinioni dei membri della rete che contribuiscono alla costruzione della conoscenza in modi dinamici, mantenendo l'apprendimento attuale attraverso il mantenimento e la cura delle reti online»

Il secondo asse sposta l'attenzione dalla centralità dell'insegnante a quella dello studente, l'efficacia «dipende dalla misura in cui il processo di apertura viene eseguito dagli insegnanti con altri insegnanti o dagli studenti supportati dagli insegnanti».

Per quanto riguarda il terzo asse, [...] una pratica può riguardare:

- Ingiustizia economica se comporta l'accesso a coloro che non potrebbero altrimenti accedere all'esperienza di apprendimento, [...] redistribuendo l'accesso, o andando oltre e ristrutturando per affrontare le cause profonde della cattiva distribuzione economica.

- Ingiustizia culturale se comporta l'accesso a coloro che non potrebbero altrimenti accedere all'esperienza di apprendimento, ridisegnando l'esperienza di apprendimento [...] riconoscendo la cultura delle minoranze».

Ingiustizia politica se va oltre il semplice accesso

all'esperienza di apprendimento e «coinvolge coloro che normalmente non hanno accesso alla riprogettazione o alla revisione dell'esperienza di apprendimento, sottolineando l'equa rappresentanza e la "parità di partecipazione" e la parità dei diritti.

Le OEP possono avere un esplicito orientamento alla giustizia sociale e l'impegno in tali pratiche rimane prezioso in quanto migliora apertamente le opportunità di accesso a pratiche pedagogiche così da consentire ad altri di poterle imparare o riapplicare»⁵.



La questione, semplificata al massimo, delle culture dominanti anche nell'ambito delle risorse aperte, risulta centrale se si vuole proporre un raggiungimento del SDG 4 davvero equo.

«Anche chi sta "ai margini" può offrire alternative alla cultura e alle pratiche dominanti costruendole sul campo [...] riconoscendo alla propria cultura, alle proprie pratiche la dignità di poter essere - alla pari di altre con maggior visibilità - foriere di cambiamenti, evoluzioni, alternative efficaci e percorribili».

È possibile integrare le pratiche di inclusione sociale attraverso i processi educativi allargando «il centro in modo che includa i margini»⁶.

L'apertura delle pratiche educative è una potente e straordinaria strategia per poter operare concretamente e dunque educare mediante una coerenza sostanziale che scaturisce dall'esempio, nei termini tuttavia di responsabilità civile e sociale, e attiva partecipazione collettiva.

4 Open Education and Social Justice, curato da Sarah Lambert, Laura Czerniewicz, Journal of Interactive Media 2 Education (2020)

5 Ibidem

6 Paola Corti, BRICKS n.5 – 2020, Allargare il centro includendo i margini

L'esigenza di un nuovo modello di design organizzativo per la gestione della crisi energetica e il rapporto fra nuove tecnologie e innovazioni legislative.

di Ludovica Zoccali*



Abstract: Gli interventi recentemente avviati dai legislatori dei vari Stati dell'Unione Europea nel c.d. settore "green" impongono al ricercatore di oggi di approfondire il rapporto fra nuove tecnologie e innovazioni legislative, al fine di poter proporre, in un futuro prossimo, un nuovo modello di design organizzativo per la gestione della crisi energetica. L'indagine deve, usufruendo di un approccio multidisciplinare e comparativistico, necessariamente muovere da un'analisi sul campo che sappia sia testare nel dettaglio i modelli aziendali esistenti sia non trascuri di tenere conto dei nuovi progressi normativi e delle nuove tecnologie volte a favorire il risparmio energetico e la riduzione dell'inquinamento ambientale..

*Dottoressa in Giurisprudenza

Negli ultimi anni, si è affermata sempre più la necessità di coordinare la gestione della crisi energetica attraverso l'analisi della transizione ecologica in ambito aziendale e legislativo, nel primo settore configurandosi la necessità di tenere conto delle nuove tecnologie volte a favorire il risparmio energetico e la riduzione dell'inquinamento ambientale mentre, nel secondo contesto, delineandosi nuove linee guida disciplinate dagli interventi recentemente avviati dai legislatori dei vari Stati dell'Unione Europea.

Pertanto, il ricercatore di oggi non può esimersi dall'approfondire lo stretto rapporto intercorrente fra nuove tecnologie e innovazioni legislative, così perseguendo il fine di proporre un innovativo modello di design organizzativo per la gestione della crisi energetica. L'indagine deve necessariamente usufruire di un approccio multidisciplinare e comparativistico nello scenario europeo, e non solo, che muova da un'analisi sul campo in grado di testare nel dettaglio i modelli aziendali esistenti ma anche, soprattutto, di integrare l'utilizzo di nuove tecnologie e inconsueti materiali ecosostenibili, volti a favorire il risparmio energetico e la riduzione dell'inquinamento ambientale, non tralasciando altresì di seguire le direttive delineate dalle più recenti produzioni legislative delle istituzioni europee.

In prima battuta, bisogna considerare l'impatto della tecnologia

sull'organizzazione aziendale - da sempre incisivo, come svela l'imporsi di nuove qualifiche professionali a ciò predisposte - che ha certamente condotto alla propagazione di nuove teorie volte a migliorare qualitativamente il design organizzativo delle aziende, essenziale per poter definire la catena di comando e la divisione del lavoro all'interno del gruppo aziendale. Basti pensare alla c.d. teoria del caos e alla c.d. teoria della learning organization. La prima percepisce le relazioni nei sistemi complessi come alimentate da interconnessioni che - quando divergenti fra loro - possono provocare effetti indesiderati, conducendo i manager e gli operatori aziendali a scontrarsi con dati imprevedibili. La seconda, invece, si pone come sua diretta conseguenza basandosi su un'interazione profonda fra i mutamenti aziendali e le risorse umane, in un'ottica di maggiore flessibilità.



Quindi, una malsana progettazione opera allorché un'azienda ricorre a metodi di organizzazione tradizionali e si pone con scetticismo nei riguardi di qualsivoglia strategia innovativa, in particolar modo nei confronti del possibile ausilio che la tecnologia potrebbe offrire nella gestione delle attività aziendali e per il miglioramento della competitività imprenditoriale, ottimizzando lo sfruttamento delle nuove risorse ecosostenibili e offrendo diversi correttivi a sostegno del malfunzionamento dei dispositivi già esistenti.

L'applicazione costante dei tradizionali metodi di design organizzativo nelle aziende garantisce stabilità nel breve periodo ma, nel lungo termine, danneggia il profilo aziendale di ciascun Paese, bloccando la creatività e il progresso. Sono diverse le realtà che difettano di applicare alla propria comunità aziendale le teorie sopracitate, fra queste l'Italia vanta un triste primato a causa dell'insufficiente e incostante ricambio generazionale all'interno della classe dirigente. Le strutture aziendali italiane precludono ai giovani manager di crescere professionalmente e le politiche occupazionali promosse da incentivi legislativi, come la riforma Treu o la legge Biagi, non hanno avuto riscontro positivo. Il mercato del lavoro è poco dinamico e l'approccio comunicativo è statico e poco multidisciplinare.

Una prima reazione alla situazione tratteggiata potrebbe scaturire dalla guida offerta dalla Strategia Nazionale di Specializzazione Intelligente (SNSI), poiché l'Agenzia per la Coesione territoriale individua le priorità di investimento di lungo periodo da condividere con i principali stakeholder, e dal Piano Nazionale di Ricerca e Resilienza (PNRR), previsto dal legislatore con il D. Lgs. n. 204/1998, che punta ad orientare la ricerca nostrana con le politiche amministrative statali e ministeriali. Il PNRR, infatti, contiene un allegato, da leggere in chiave di ricerca e innovazione, interamente dedicato al clima, all'energia e alla mobilità sostenibile, con un approfondimento relativo anche all'energetica industriale.

In tale scia, nello scenario europeo, si colloca il c.d. React-Eu (Assistenza alla ripresa per la coesione e i territori d'Europa), piano finanziario volto a prevedere misure per favorire la c.d. ripresa verde e la crisi dovuta alla pandemia da Covid-19, entrata in vigore il 24 dicembre 2020 e decorrente, retroattivamente, dal 1° febbraio 2020 al 31 dicembre 2023 (Regolamento UE 2020/2021 del Parlamento

Europeo e del Consiglio Europeo del 23 dicembre 2020).

Ad esempio, l'ordinamento tedesco offre importanti spunti di riflessione, specie in tema di conservazione dell'ecosistema, biodiversità, riduzione degli impatti del cambiamento climatico e promozione di uno sviluppo sostenibile.

La Germania è leader in Europa e nel mondo in materia di energie rinnovabili, grazie alla riforma della legge EGG (Erneuerbare Energien Gesetz), con cui si pone l'obiettivo di raggiungere la neutralità dei gas ad effetto serra entro il 2050, in linea con il Green Deal Europeo, programma proposto dalla Commissione Europea allo scopo di raggiungere la neutralità climatica entro i prossimi decenni e, conseguentemente, volto a spronare tutti i Paesi dell'Unione Europea ad innovare le proprie leggi in materia di economia circolare, biodiversità e ristrutturazione degli edifici.

La decarbonizzazione dell'economia, in termini di maggiore circolarità, è realizzabile anche in Italia, supportando lo sviluppo di materiali innovativi ecocompatibili e riducendo l'attuale sistema della produzione di plastiche, fortemente dipendente da materie prime fossili non rinnovabili e non riciclabili in maniera ottimale, e facendo tesoro di alcuni punti di forza, come il già avviato passaggio agli usi stazionari al gas e alle nuove tecnologie, nel settore industriale, e la centralità della posizione geografica. Un'altra soluzione al problema della semplificazione del design organizzativo aziendale italiano potrebbe provenire da una riqualificazione delle tendenze aziendali e da nuove politiche di formazione, che puntino a riformare i sistemi scolastici e universitari in maniera incisiva, come già accade all'estero, in Europa (ad es., Regno Unito) e non solo (ad es., Stati Uniti d'America e Australia).

La proposizione di un nuovo modello di design organizzativo deve consentire ai ricercatori, ai manager e ai giuristi del domani di conseguire una elevata professionalità in ambito aziendale tale da dominare la governance del cambiamento climatico e della crisi energetica, non ignorando, tuttavia, che il progresso non necessita solo di uno statico apprendimento – ossia di una mera condivisione del sapere - ma soprattutto di creatività, aspetto più dinamico dello stesso sapere.

FONTI NORMATIVE

- Legge delega n. 196/1997
- D. Lgs. n. 280/1997
- D. Lgs. n. 468/1997
- D. Lgs. n. 204/1998
- Legge n.30/2003
- Regolamento UE 2020/2021 del Parlamento Europeo e del Consiglio Europeo del 23 dicembre 2020
- EGG (Erneuerbare Energien Gesetz)

SITOGRAFIA

- [http://www.italoeuropeo.com/2011/10/30/la-teoria-del-caos-lingrediente-che-manca-allitalia/;](http://www.italoeuropeo.com/2011/10/30/la-teoria-del-caos-lingrediente-che-manca-allitalia/)
- [https://www.edilportale.com/news/2021/02/aziende/fonti-rinnovabili-nuove-leggi-in-germania-e-possibilita-di-ripresa-in-italia_80823_5.html.](https://www.edilportale.com/news/2021/02/aziende/fonti-rinnovabili-nuove-leggi-in-germania-e-possibilita-di-ripresa-in-italia_80823_5.html)



ROBOTICA COLLABORATIVA

di Paolo Preianò*

Astract: *In questo articolo si parlerà di robotica collaborativa specificando i possibili scenari futuri, gli studi del settore e il loro stato di avanzamento, i rischi che potrebbero sorgere nei prossimi anni soprattutto nel campo della salute e sicurezza sui luoghi di lavoro. Si tratta di un tema particolarmente delicato oggetto anche di una specifica standardizzazione da parte della ISO.*

*Ingegnere - Esperto Sicurezza sul Lavoro

C'era una volta un ragazzotto universitario in preda all'ansia da esame, studente di ingegneria al primo anno di specialistica ed un docente di robotica industriale, genio assoluto della materia con il classico physique du rôle consolidato dalla convenzione (capelli incolti, abbigliamento discretamente trasandato, ufficio olezzante di tabacco e caffè ecc.). L'esame constava nella modellizzazione e poi nella programmazione di un piccolo movimento di un end effector di un robot da laboratorio: si tratta di spostare un oggetto sferico da un punto A ad un punto B. Il docente, dopo aver esaminato il giovane per un'oretta circa, dopo averlo promosso, gli pone una domanda: "Mi dica: lei che futuro vede in tema di diavolerie del genere?". Per chi ancora non l'avesse capito si tratta di un racconto autobiografico e posso assicurarvi che quella fu la domanda più tosta di tutto l'esame anche se era esterna ad ogni valutazione. Tuttavia, e chi l'ha vissuto sa benissimo, la fase successiva al superamento dell'esame è caratterizzata da una strana euforia, una scarica di adrenalina che ti rende più sfacciato, con quel mix di felicità e menefreghismo piacevole in alcuni contesti come quello. Fu esattamente quella condizione che rese il discorso surreale:

"Professore, secondo me un domani noi finiremo a guardare questi attrezzi che faranno tutto al posto nostro. Magari cresceranno i lavori come il suo ma caleranno quelli meno qualificati e la cosa non mi piace per nulla."

Il prof. fece una leggera smorfia col viso, di quelle che faceva prima di bocciare (un movimento delle sopracciglia che nessuno era in grado di imitare), e disse:

"Si segni questo termine: robotica collaborativa. Non le spiego di cosa si tratta, approfondisca lei".

"Veramente professore ho paura che un domani, se non si sta attenti, anche noi saremo sostituiti da questi amici di latta".

"Sì, lo diceva anche mio nonno quando gli feci vedere

il primo PC. Eppure siamo qui io e lei a fare un esame e di fronte a lei non c'è un programma, ci sono io in carne ed ossa. Lei pensa che una macchina avrebbe potuto esaminarla meglio di me?".

Domanda a trabocchetto, pensai. Ancora doveva firmare il libretto degli esami per cui non ebbi esitazione a rispondere, mentendo come neanche Paolo Villaggio avrebbe saputo illustrare nei suoi dipendenti fantozziani:

"No, assolutamente".

"Ora vada perché ho altri suoi colleghi da esaminare". Per molto tempo quel termine continuò a girovagare per la mia testa. Robotica collaborativa, che sarà mai? Qualche mese fa, nel corso di una videoconferenza con alcuni colleghi, quel concetto riaffiorò quando uno dei tecnici iniziò a parlare della convivenza dei robot con i lavoratori e di quanto sia necessario mettere in campo delle misure di tutela per la loro salute e sicurezza da quelli che potrebbero essere azioni abnormi da parte di una macchina. Proust avrebbe chiamato quel richiamo memoria involontaria come l'arcinota madeleine che tutti quanti avranno sentito menzionare nel corso dei loro studi. Cerchiamo allora di vedere insieme cosa è la robotica collaborativa e quali implicazioni potrebbe avere sul lavoratore e con ciò dare merito al docente dell'incipit che non si ricorderà neanche della mia faccia, figurarsi del dialogo.

Con "robotica collaborativa" ci si riferisce a quei sistemi robotici di nuova generazione che sono in grado di interagire fisicamente e in sicurezza con l'uomo e di dividerne lo spazio, non rimanendo pertanto più confinati in una "gabbia" che separa lo spazio dell'uomo da quello del robot. "Fisicamente" e "in sicurezza" sono i due punti sui quali insiste il mio lavoro quotidiano e quello dei tanti colleghi ingegneri della sicurezza. Quando possiamo dire che due soggetti – macchine o umani oramai stiamo imparando a non fare differenza – condividono uno spazio "in

sicurezza”? Diciamo subito che la condivisione dell’ambiente di azione, altrimenti detta interferenza, non è solo di tipo spaziale ma anche temporale. Un cantiere nel quale agiscono, anche in due momenti differenti, due soggetti afferenti ad aziende diverse, hanno il potenziale di interferire. Facciamo un esempio: nella costruzione di un edificio interviene una ditta per l’intonacatura interna, finisce il lavoro e va via. Il giorno seguente l’elettricista va sullo stesso posto per posare dei cavi o un quadro. L’azione del primo soggetto modificherà lo stato dei luoghi, gli operai potrebbero ad esempio lasciare detriti o materiale che andrebbero a introdurre altri rischi dei quali il secondo soggetto deve essere informato per azionare le misure di prevenzione e protezione adeguate. Questo aspetto è molto importante perché, mentre si comprende facilmente l’interferenza spaziale (due soggetti diversi sullo stesso posto), quella temporale (due soggetti sullo stesso posto non contemporaneamente) è molto trascurata. Dicevamo dunque: convivenza in sicurezza. L’interazione uomo-macchina, detta in termini anglosassoni Physical Human-Robot Interaction (PhHRI), richiede che il robot abbia la comprensione di 2 fattori:

- l’ambiente nel quale agisce insieme all’essere umano;
- la previsione dell’intenzione umana.

Il secondo aspetto è un po’ inquietante. Può mai una intelligenza artificiale avere un modello predittivo sull’agire umano? In che modo questo potrebbe essere usato contro l’uomo? La risposta alla prima domanda è “sì, certamente” e ne sono esempi le note sfide a scacchi che le IA hanno intavolato con successo contro le intelligenze umane. Proprio queste si basano esattamente sulla previsione delle mosse dell’avversario. Riguardo alla seconda potremmo richiamarci ai principi base di un robot che furono teorizzate anni fa dal pioniere Isaac Asimov del quale abbiamo parlato tanto su queste pagine e che si basano sull’importanza di una macchina di rimanere fedele agli ordini impartiti dall’essere umano e di inibire ogni possibile azione lesiva nei confronti di quest’ultimo. Si viene a costituire un binomio uomo-robot dove le due entità operando insieme beneficiano mutuamente dell’azione coordinata di entrambi. In un tale contesto la macchina solleva l’uomo dalle azioni gravose e abbiamo già visto, in precedenti articoli alcuni casi come quello degli esoscheletri, contemporaneamente, beneficiare delle abilità dell’uomo stesso prevedendo e risolvendo in

anticipo situazioni imprecise, modellando la propria azione (campo di azioni) per rendergli la vita più facile.

È chiaro che progettare un cantiere o un luogo di lavoro in generale con questi termini prevede un cambio di paradigma che, se fatto bene, e qui interviene il lavoro di un ingegnere per la sicurezza, conduce a importanti migliorie per quanto riguarda ad esempio la sostenibilità, la resilienza e la centratura sull’uomo di un sistema del genere. “L’uomo al centro” è il motto della nostra rivista e della sensibilizzazione quotidiana che cerchiamo di apportare, ma è anche quello che ogni legge ben fatta ed ogni azione seria dovrebbe possedere senza alcun ragionevole dubbio. Usare la tecnologia per dare valore all’uomo. L’idea molto interessante, sostenuta dalla comunità scientifica, è quella di consentire una collaborazione proattiva con trasferimento di capacità tra esseri umani e robot con una sorta di mutuo miglioramento che potrebbe (condizionale d’obbligo) rendere la prossima generazione degli automi con maggiore capacità di azione e con minore necessità di supervisione umana oltre che con capacità cognitive, sociali e tecniche efficienti sempre e solo con l’unico fine di assistere ed interagire in sicurezza con l’essere umano. Questa non è la concezione di un singolo esperto. Si tratta della visione della IFR – International Federation of Robotics che nel suo position paper sul potenziale impatto della robotica sul mondo del lavoro prevede la creazione di nuove competenze per agire sulla parte immateriale del confronto tra le due realtà che, dovremo abituarci, a veder coesistere per il futuro lasciando magari da parte ogni dubbio.

Senza che ce ne accorgessimo, negli ultimi anni la robotica collaborativa è entrata a pieno titolo in diverse aziende divenendo anche oggetto di uno standard specifico da parte della ISO. Si tratta dello standard ISO/TS 15066, che definisce i requisiti di sicurezza della robotica collaborativa. Come abbiamo sempre detto la quarta rivoluzione industriale rappresenta l’evoluzione dell’industria verso un modello intelligente in cui robotica (collaborativa), interfaccia uomo/macchina, digitalizzazione, big data e artificial intelligence sono messe nello stesso calderone e fuse insieme per dare un prodotto unico: un sistema lavorativo che da un lato riduce i rischi e gli infortuni sul lavoro (a proposito: anno terribile il 2021!) e dall’altro preserva la centralità dell’uomo in maniera sicura e permettendo scambi proficui. Alla robotica collaborativa si riconoscono alcuni innegabili meriti:

velocizza i processi industriali più ripetitivi, è flessibile, è sicura ed è di facile utilizzo, non richiede infatti conoscenze di programmazione approfondite. Inoltre, diversamente da quanto si sarebbe portati a pensare, comporta investimenti tutto sommato sostenibili.

La cosa più importante è tenere separati i 2 universi. Le macchine sono macchine, gli uomini sono uomini. Le prime sono soggette a obsolescenza, i secondi no. Almeno si spera.

BIBLIOGRAFIA

<https://www.agendadigitale.eu/industry-4-0/robotica-collaborativa-perche-e-la-chiave-per-lindustria-5-0/>

<https://www.sick.com/it/it/robotica-collaborativa-la-rivoluzione-dellindustria-40/w/blog-it-robotica-collaborativa/>



Pensiero computazionale: imparare a sviluppare strategie fin da bambino

di Davide Sorrentino*

Astratt: I concetti dell'informatica rientrano nella nostra cultura di base, insieme alla letteratura, alla matematica, alla biologia, alla storia, etc. Per le nuove generazioni (noti come "nativi digitali") la programmazione informatica (coding) è fondamentale per aiutare a capire il funzionamento delle tecnologie, in modo da diventare soggetti attivi della tecnologia.

*Ingegnere - Esperto in sicurezza informatica

Quando affrontiamo problemi complessi ricercando soluzioni che prevedono più fasi per il completamento dell'obiettivo, stiamo applicando il pensiero computazionale. Il pensiero computazionale può essere definito come "l'insieme dei processi mentali coinvolti nel formulare problemi e le loro soluzioni in modo che le soluzioni possano essere rappresentate in una forma che possa essere efficacemente eseguita da un agente di elaborazione dell'informazione" [1]. Tale definizione non deve farci pensare che bisogna ragionare come un programmatore o, peggio, come un computer.

La International Society for Technology in Education (ISTE) e la Computer Science Teachers Association (CSTA) hanno definito formalmente il pensiero computazionale come un processo di risoluzione dei problemi che include le seguenti caratteristiche:

- formulare i problemi in modo da poter utilizzare un computer e altri strumenti elettronici/informatici per favorire la risoluzione;
- organizzare e analizzare i dati in modo logico;
- rappresentare i dati attraverso modelli matematici e simulazioni;
- automatizzare le soluzioni attraverso degli algoritmi;
- identificare, analizzare e implementare le possibili soluzioni cercando di raggiungere l'ottimo, cioè ricercando la combinazione di risorse e l'algoritmo più efficace;
- generalizzare il processo di risoluzione dei problemi, in modo da applicarlo ad un'ampia varietà di problemi simili.

Quando applichiamo il pensiero computazionale?

In prima analisi, il pensiero computazionale è sempre

applicato dai programmatori e dai progettisti (es. la stesura di un codice, la progettazione di robot più o meno complessi, etc.) ma non si ferma solo a questi settori. Quotidianamente ognuno di noi applica il pensiero computazionale, ad esempio quando seguiamo istruzioni per il montaggio di un mobile, quando ragioniamo su quale sia il percorso migliore per rientrare a casa o quando un bambino sceglie i colori per disegnare.

In altri termini, il paradigma informatico può (anzi deve!) essere applicato anche al di fuori dell'ambito informatico per insegnare agli studenti a risolvere problemi complessi.

Perché insegnare la programmazione informatica?

La programmazione non deve essere il fine ma il mezzo per sviluppare delle strategie, per ipotizzare soluzioni che prevedono più fasi (o passi), per capire l'importanza di una comunicazione e di una descrizione chiara ed univoca in modo da capire cosa fare e quando procedere.

Per maggior chiarezza, supponiamo di dover montare un mobile acquistato da Ikea. Le istruzioni fornite dal produttore costituiscono gli strumenti per la soluzione del problema (lo scopo), cioè montare l'oggetto, e sono scritte in modo ordinato e logico in modo che, seguendo tutti i passi si arriva alla soluzione del problema. Si può affermare, quindi, che le istruzioni costituiscano un vero e proprio algoritmo perché non solo permettono all'utente di raggiungere lo scopo ma consentono anche ad altri utenti la risoluzione del problema nel caso in cui debbano montare prodotti simili.

Insegnare il coding è importante per svariati motivi, tra cui:

- stimola gli studenti a creare contenuti, trasformandoli in utenti attivi e non solo

fruttori;

- permette agli studenti di sbagliare in modo sicuro e costruttivo, cioè di autocorreggersi e migliorarsi studiando i propri errori;
- consente di mettere in pratica i principi della matematica studiati;
- stimola il lavoro di squadra e la collaborazione con gli altri compagni.

BIBLIOGRAFIA E SITOGRAFIA

- [1] Wing J. M., *Computational Thinking, Communications of the ACM*, Marzo 2006/Vol. 49 No. 3, pg 33-35
- [2] <https://www.ctsprato.edu.it/wp-content/uploads/2017/03/dal-coding-alla-robotica.pdf>
- [3] <https://www.pensierocomputazionale.com/2020/02/24/tinkercad-ovvero-modellare-in-3d-con-il-coding/>
- [4] <https://iceral.edu.it/wp-content/uploads/2020/10/robotica6.pdf>
- [5] <https://unsplash.com/photos/KgLtFCgfC28>

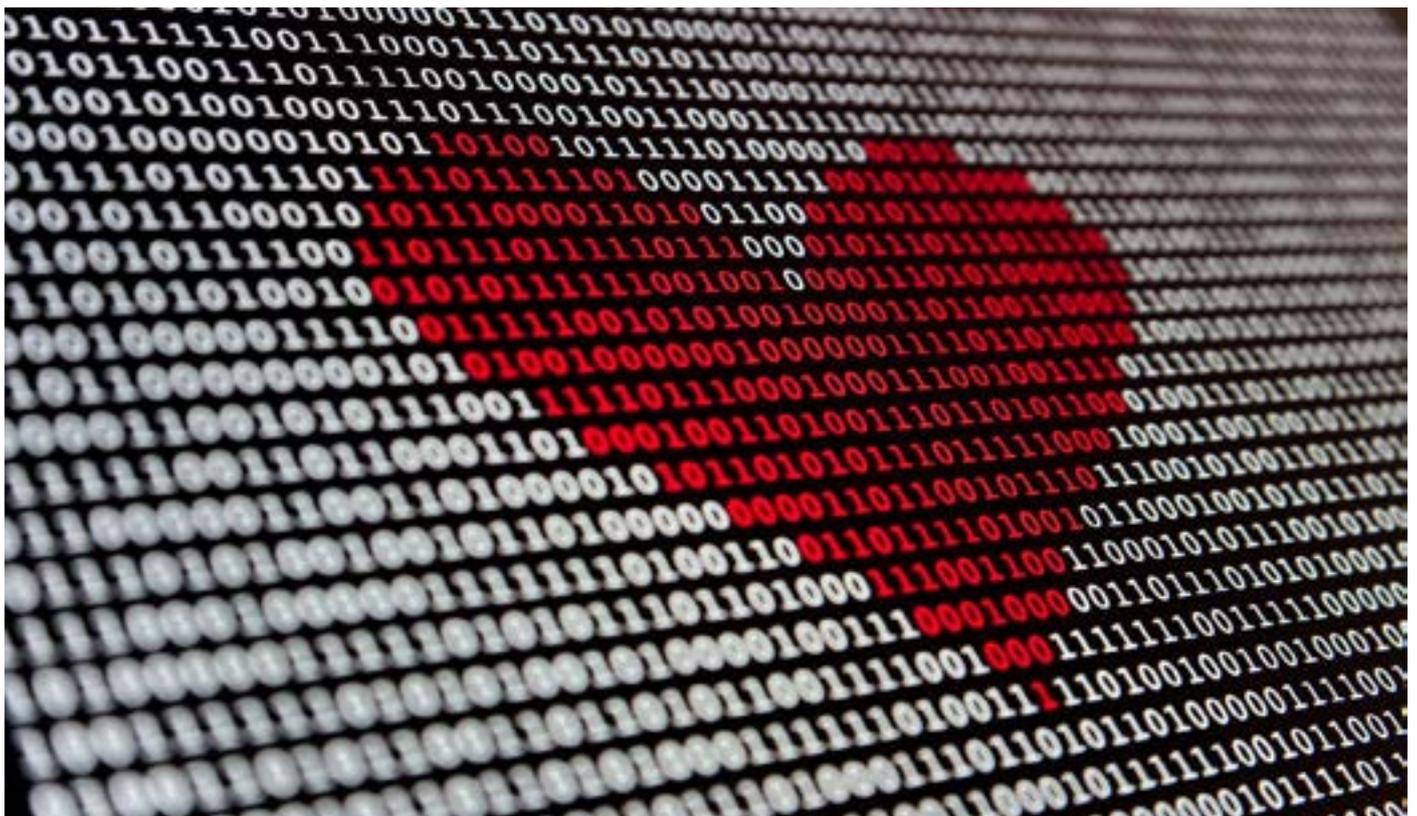
La robotica educativa

La robotica educativa, nata con finalità didattiche, aiuta a ragionare in maniera logica (algoritmica) sui problemi e sui sistemi. Rispetto alla sola programmazione, la robotica permette di ragionare su un qualcosa di tangibile e pratico, applicando in modo efficiente la programmazione informatica.

Conclusioni

La nostra epoca si evolve in modo repentino, spesso senza che vi sia la possibilità di capirne i meccanismi. Fra i requisiti più richiesti nel mondo del lavoro spicca su tutte la conoscenza dei principali software per PC ed il futuro non può non essere tecnologico perché ogni evoluzione viene fatta sfruttando soprattutto la tecnologia.

È fondamentale che i ragazzi sviluppino un pensiero computazionale perché saranno loro a dover costituire le basi fondamentali della nuova società.



LOG4SHELL

di **Benedetto Fucà***



Cos'è Log4Shell, una delle più grandi vulnerabilità riscontrate di recente e che sta creando gravi problemi sulla rete e sugli applicativi che racchiudono questa vulnerabilità. Questa minaccia rischia di mettere a dura prova la sicurezza dei sistemi informatici aziendali, non

tanto per le azioni di rimedio da porre in essere, ma perché la superficie d'attacco potenziale è talmente vasta che richiede, in prima battuta una fase di mappatura per capire quali software contengono questa vulnerabilità. E se da un lato aziende strutturate possono permettersi di ricorrere ai ripari attraverso i reparti IT, piccole aziende rischiano di trovarsi impreparate e facili prede, con conseguenze notevoli per via della peculiarità della vulnerabilità.

L'Agenzia Italiana per la Cybersecurity, il 10 dicembre 2021, ha lanciato sul proprio sito un Proof of Concept (PoC) identificando una vulnerabilità grave relativa al prodotto Apache Log4j. Si tratta di una vulnerabilità zero-day, all'interno del modulo open source Log4j di Apache Project. Uno dei framework di logging, più utilizzati, scritto in Java e distribuito da Apache Software Foundation che gli sviluppatori utilizzano per tenere traccia dell'attività del software nelle app cloud e aziendali.

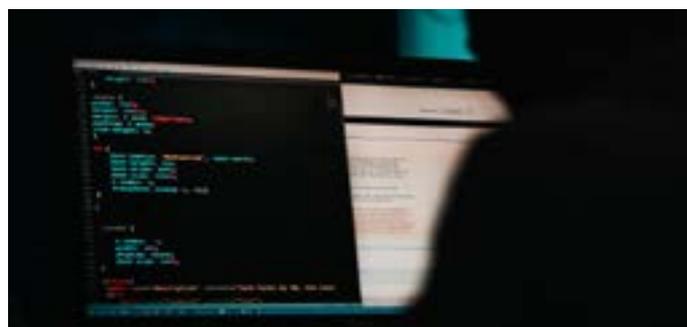
Secondo gli esperti, si tratta della più grande falla degli ultimi decenni che sta causando gravi problematiche a moltissime aziende che utilizzano software scritti con questa libreria. Questa falla, denominata Log4j 2, permette a chiunque abbia un minimo di esperienza con i computer di attaccare infettare e sfruttare questa vulnerabilità per prendere il controllo di un sistema infetto. La criticità di tale vulnerabilità è stata classificata dallo CSIRT con un valore d'impatto pari al valore Grave/Rosso., mentre l'agenzia MITRE l'ha classificato con un valore 10 su una scala di 10.

Nella nota pubblicata dall'Agenzia per la Cybersecurity, del 12 dicembre 2021, si riporta che sussiste *“la presenza di una vasta e diversificata superficie di attacco sulla totalità della rete e*

considerando la sua semplicità di sfruttamento, anche da parte di attori non sofisticati, rende la segnalata vulnerabilità particolarmente grave”.

Questa vulnerabilità è stata scoperta dopo che sono stati compromessi, per primi, i server del noto videogioco Minecraft, dove alcuni giocatori hanno iniziato a mandare delle stringhe di testo del codice per sfruttare la suddetta vulnerabilità. Ma non è solo il noto videogioco ad essere preso di mira: Twitter, Amazon, LinkedIn, Apple e molti altri sistemi possono essere aggrediti sfruttando questa vulnerabilità. Secondo, gli esperti, dal momento in cui è stata resa pubblica, gli attacchi che sfruttano questa criticità sono cresciuti in maniera esponenziale; il Check Point Research ha registrato *“oltre 100 hack al minuto, 200.000 attacchi dopo 24 ore dalle rilevazioni iniziali, che sono diventati 800.000 dopo 72 ore, e a cui ne vanno aggiunti altri 40.000 registrati solo sabato scorso”.*

Si stima che oltre 90 Paesi in tutte le regioni del mondo e oltre il 60% delle reti aziendali risultano colpite. In Italia la situazione si manifesta con oltre il 43% delle reti aziendali che hanno subito un tentativo di exploit. Analizzando le modalità con cui essa viene sfruttata, si nota che la maggior parte degli attacchi si concentrerebbe sull'installazione di estrattori di cryptovalute e tentativi di attacchi per distribuire Trojan, Botnet e Ransomware, questi ultimi sempre più utilizzati per rubare dati sensibili, documenti di identità, contratti e chiedere riscatti. Secondo quanto sostenuto dai ricercatori di Bitdefender, i criminali informatici stanno tentando di diffondere Khonsari, una nuova famiglia di ransomware, per colpire i sistemi basati su Windows e il Trojan (RAT) di accesso remoto Orcus. La maggior parte dei primi attacchi finora ha preso di mira i server Linux e sarebbero principalmente di *“reverse bash shell”*, tecnica utilizzata per guadagnare un punto d'appoggio





nei sistemi per sfruttarli in un momento successivo. Inoltre, sarebbero molte e diversificate applicazioni che utilizzano il framework in esecuzione su sistemi operativi come Windows, Linux, macOS e FreeBSD. Java, inoltre, alimenta web cam, sistemi di navigazione per auto, lettori DVD e set-top box, vari terminali e persino parchimetri e dispositivi medici. Di conseguenza, questa vulnerabilità potrebbe avere un effetto catena molto significativo e risulta difficile prevedere la portata totale e l'impatto a lungo termine della vulnerabilità.

Allo stato attuale, Apache ha rilasciato già la terza patch, dopo che le prime due rilasciate avevano al loro interno altre vulnerabilità. La problematica non sta nella difficoltà di andare a "riscrivere" il codice, quanto nel fatto che sono quasi tutte le applicazioni che si trovano all'interno di un perimetro aziendale che sono colpite e questo fa sì che ci sia dietro un lavoro meticoloso.

Allo stato attuale, gli esperti consigliano non solo di seguire gli aggiornamenti di patch ma di effettuare back-up di dati personali, in modo tale da poter avere sempre una copia in caso si subisse un attacco.

Questa vulnerabilità deve far riflettere sulla sempre più dipendenza dai sistemi informatici che a sua volta deve essere accompagnata da una cultura della sicurezza che pone il dato al primo posto. Il rischio che questa vulnerabilità venga sfruttata dagli hacker è sotto gli occhi di tutti, e se da un lato, aziende robuste composte da un reparto IT proattivo e aggiornato sul tema possono limitare le conseguenze di questa vulnerabilità; il discorso si complica per aziende

piccole che hanno adottato applicazioni che vanno ad impattare il proprio business e che contengono questa vulnerabilità che ha come caratteristica quella di sfruttare e andare ad impattare sui log.

Infatti, gli aggressori possono inviare richieste in cui le intestazioni HTTP sono "spruzzate" con stringhe dannose, costruite per stuzzicare l'applicazione ricevente nell'esecuzione della sostituzione del messaggio, a quel punto l'applicazione attiva la vulnerabilità e carica o esegue il codice remoto.

Secondo gli esperti, nonostante tale vulnerabilità venga sanata, la grossa mole di attacchi che sono stati portati avanti durante questa fase, comporterà delle ripercussioni notevoli che protrarranno i propri effetti anche nel lungo-medio periodo. Questa situazione è dovuta anche dal fatto che, come detto sopra, sfruttare questa vulnerabilità richiede competenze basilari, la superficie delle applicazioni che potenzialmente possono essere attaccate è notevole ed inoltre è difficoltoso andare ad intervenire su ciascuna delle singole applicazioni, senza il rischio che venga dimenticata qualcuna.

Ma la problematica investe anche il modo con cui si va a scrivere un determinato codice, sfruttando librerie open source e quindi lo sviluppo del software, aprendo un dibattito alla luce di quella che può essere definita come la più grande falla IT.

***Assistant IT Risk Advisory
Laurea in Giurisprudenza e
Master in Cyber security
Digital Forensic & Computer Crime**

Lo Spear phishing e l'utilizzo di nuove tecniche con la social engineering

di Andrea Cortese*



Astract: Il phishing è in continua evoluzione grazie allo sviluppo di nuove tecniche di attacco che sono nate negli ultimi anni con l'obiettivo di rubare dati personali e compromettere sistemi informativi aziendali. I sistemi di intrusion detection and prevention non costituiscono una soluzione definitiva e per questo è necessario un utilizzo combinato di servizi perimetrali di sicurezza con la formazione e l'educazione alla sicurezza informatica del personale dell'organizzazione.

Secondo il Rapporto Threat Landscape 2020 dell'ENISA, l'Agenzia Europea per la CyberSecurity, il phishing si colloca al terzo posto tra le principali minacce informatiche per le organizzazioni e le persone dopo i Malware e gli attacchi Web-based. Un fenomeno che ha raggiunto un picco di quasi 250 mila attacchi in Europa nel mese di gennaio di quest'anno e che nel 2019 ha prodotto 26,2 miliardi di perdite con la compromissione delle e-mail aziendali¹.

*Area Tecnico – Scientifica ed elaborazione dati - Università degli Studi di Napoli Federico II

1 European Union Agency for Cybersecurity (ENISA). (2020). Threat Landscape – 2020 Phishing.

La tendenza degli attacchi è in continuo aumento anche nel nostro Paese: già nel 2019 la Clusit, l'Associazione italiana per la sicurezza informatica, segnalava un incremento esponenziale del fenomeno e in particolare – aspetto particolarmente preoccupante – una continua e costante evoluzione dello stesso con la nascita di nuove tecniche che vanno di pari passo con lo sviluppo tecnologico, inteso in termini di IA e capacità di elaborazione e calcolo². Inoltre, ci sarebbe da aggiungere anche un ulteriore fattore, non meno importante, che contribuisce all'evoluzione del phishing: le ragioni di carattere politico-strategico nell'ambito delle azioni condotte da alcuni Paesi in termini di politica di cyber-spionaggio civile, militare e industriale.

Anche Microsoft nel suo rapporto annuale, il Security Intelligence Report³, sottolinea come il phishing, nel variegato mondo delle minacce informatiche, rappresenti il metodo di attacco preferito in quanto si fonda su due aspetti umani: quello di compiere dei giudizi e di prendere delle decisioni. Prima di procedere all'approfondimento dello Spear Phishing si rende necessario chiarire, senza alcuna pretesa di completezza, cosa sia il phishing e in particolare quali siano le principali classificazioni sulla base delle



tipologie di attacchi.

Secondo la definizione data da Cisco, il “phishing è il tentativo fraudolento di rubare i dati degli utenti, come credenziali di accesso, dati della carta di credito o anche denaro, mediante tecniche di ingegneria sociale. Questo tipo di attacco viene in genere lanciato attraverso messaggi di posta elettronica che sembrano inviati da una fonte attendibile, con l'intento di convincere l'utente ad aprire un allegato malevolo o a seguire un URL fraudolento”⁴.

Tra le principali classificazioni di phishing sulla base

² Associazione italiana per la sicurezza informatica (CLUSIT). (2019). Rapporto Clusit 2019 sulla sicurezza ICT in Italia.

³ Microsoft Corporation. (2021). Microsoft Digital Defense Report.

⁴ «What Is Phishing?». Cisco. <https://www.cisco.com/c/en/us/products/security/email-security/what-is-phishing.html>

delle tipologie di attacco possiamo distinguere:

Domain Impersonation, si tratta del classico phishing di massa dove il dominio del messaggio è simile a quello originale. Il testo dell'e-mail in genere presenta degli errori ortografici. Gli aggressori tentano di impersonificare il dominio dell'azienda legittima utilizzando tecniche come il typosquatting che consiste nella sostituzione di una o più lettere di un dominio di posta elettronica con lettere simili o in domini di primo livello diversi da quello legittimo (ad es: invece di `ibm.com`, `ibm.co`).

Domain Spoofing, viene falsificata l'identità del mittente mediante l'utilizzo di un dominio originale e legittimo del quale il sito fraudolento prende le sembianze. L'indirizzo del mittente è quindi costituito da un dominio legittimo, ciò rende particolarmente difficile distinguere l'e-mail falsa da quella reale.

Phishing Attachments, in tal caso il messaggio contiene un allegato, un documento Word, un file zippato, un excel o addirittura un eseguibile .exe che se eseguito può comportare una seria compromissione del sistema mediante l'apertura di porte a malware.

User Impersonation, in tale tipologia viene camuffato l'indirizzo e-mail del mittente dietro un'identità familiare e nota al destinatario del messaggio al fine rafforzare la convinzione circa l'autenticità del messaggio e indurre l'utente a cliccare su link.

Credential Phishing Links, l'e-mail contiene il link a pagine che somigliano ad alcuni siti web legittimi, come banche o istituzioni pubbliche, social network, provider o aziende importanti. L'apertura del link porterà ad un sito web, un loading page, che avrà un aspetto familiare o simile a quello legittimo. Inserendo i propri dati nel falso form questi verranno copiati al fine di riutilizzarli per furti d'identità o transazioni bancarie.

Tali classificazioni, in ogni caso, non devono essere considerate in modo rigido, in quanto, nella stragrande maggioranza dei casi gli spammer, o meglio i phisher, utilizzano diverse combinazioni di tali tecniche. Adempio, un phishing che trasmetteva una falsa fattura TIM lanciato nel 2017 utilizzava una combinazione di diverse tecniche di Domain Spoofing, Phishing Attachments e Domain Impersonation.

In questo esempio, possiamo vedere i loghi legittimi della Telecom Italia e TIM, un utilizzo di testo in

italiano e l'allegato fattura in formato zip. Si tratta, quindi, di un insieme di tecniche che hanno come



obiettivo quello di rendere credibile la comunicazione. L'indicazione del numero di fattura, l'avviso relativo alla sola trasmissione online del documento sono ulteriori elementi che fanno pensare all'autenticità della stessa. Unico elemento di sospetto, in quanto non viene utilizzato un domain spoofing ma solo un domain impersonation, è dato dall'indirizzo e-mail del mittente.

Spear phishing e social engineering

Una particolare tipologia di phishing particolarmente efficace, in quanto utilizza tecniche di ingegneria sociale, è quello della spear phishing. Si tratta di una particolare forma di phishing che non utilizza un format standardizzato per una trasmissione massiva (il c.d. spray phishing), la comunicazione viene studiata invece per essere indirizzata ad una specifica organizzazione o ad una specifica persona, come ad esempio il capo di un'azienda. Essa, inoltre, utilizza la leva della risposta emotiva al fine di indurre gli utenti ad adottare l'azione.

Il phisher utilizza quindi tecniche di ingegneria sociale che consistono nello studio dell'organizzazione aziendale o della struttura pubblica al fine di costruire una comunicazione convincente, che dia poco spazio a valutazioni di carattere personale e che necessiti di un'azione quanto più immediata possibile. L'azione tipica è quella di cliccare su un link e di compilare un form con le proprie credenziali personali. L'immediatezza dell'azione è resa necessaria in quanto l'e-mail comunica che possono essere compromesse delle funzionalità in caso di inerzia dell'utente, come ad esempio la scadenza di un account o di una password, un riempimento della propria casella di posta elettronica o la conferma entro poche ore della validità dei propri dati pena la disattivazione dell'account.

Definito il messaggio e strutturata la comunicazione essa viene quindi resa credibile mediante l'utilizzo di un format tipico adottato dall'organizzazione frutto del lavoro di studio, come ad esempio l'utilizzo di caratteri, di colori o di uno stile specifico. Ad esempio, viene utilizzato il logo dell'azienda o della struttura. Una tecnica ingegneristica può consistere nella registrazione alla newsletter al fine di comprendere lo stile comunicativo, il contatto telefonico preventivo al fine di carpire informazioni sui ruoli, mansioni o processi che non sono immediatamente comprensibili tramite il sito web. Ad esempio, per estrapolare informazioni sul formato di layout dell'e-mail i phisher contattano il servizio clienti per presentare false proteste o chiedere semplicemente delle informazioni.

Pertanto, l'utilizzo di una firma, con il nome, cognome e qualifica, di un appartenente all'organizzazione che rivesta realmente un ruolo di specifico, preferibilmente di prestigio – si pensi ad un dirigente o un capo – è il risultato di un'analisi attenta, certamente non condotta in modalità standardizzata. In alcuni casi, il prelievo di tali informazioni è un vantaggio che è stato offerto, in particolare nella Pubblica Amministrazione, dagli obblighi di trasparenza amministrativa. Le norme, infatti, obbligano le PA a rendere pubblici i nominativi dei dirigenti e dei responsabili dei diversi uffici che compongono la struttura.

L'aggiunta di un numero di telefono apparentante all'organizzazione, eventualmente non diretto della persona indicata, al fine di rendere più complessi i contatti ricostruzione della veridicità della comunicazione e l'utilizzo di Domain Spoofing per mascherare e l'indirizzo del mittente completano il quadro rendendo l'e-mail particolarmente convincente. Può contenere un allegato o semplicemente un link verso un sito esterno camuffato con l'inserimento del dominio legale all'interno dell'url (ad esempio www.dominiodiphishing.ru/ www.dominioazienda.it/).

Tale tipologia di phishing può essere condotta verso una singola persona, nei confronti di tutta l'organizzazione o parte di essa, ma in ogni caso l'obiettivo finale è sempre di rubare credenziali, installare malware come ransomware, o dare avvio ad attacchi più complessi.

I consigli degli esperti

In termini generali, le organizzazioni, a livello

tecnico - secondo il rapporto ENISA - dovrebbero certamente utilizzare gateway e-mail di sicurezza con manutenzione regolare (eventualmente automatizzata) dei filtri (antispam, anti-malware, filtraggio basato su policy), tuttavia, i sistemi di identificazione e prevenzione, non sono sempre sufficienti. Si rende necessaria anche un'adeguata formazione del personale nel riconoscere le e-mail fraudolente, anche mediante l'utilizzo di test di simulazione per mettere alla prova l'infrastruttura dell'organizzazione e la reattività del personale. Esattamente come avviene nelle esercitazioni per la sicurezza sui luoghi di lavoro. Anche l'utilizzo di antivirus installati sui PC-workstation del personale non è sempre la soluzione definitiva, si pensi a coloro che leggono la posta di lavoro dal cellulare aziendale oppure su client di posta tramite browser.

Con particolare riferimento allo spear phishing, alcuni suggerimenti da parte delle maggiori aziende di sicurezza informatica sono volti a consigliare l'utilizzo di protocolli di sicurezza in azienda, la creazione di canali di comunicazione interna sicuri, la verifica della legittimità dei mittenti, l'utilizzo di password diverse per gli account aziendali e personali⁵.

42,8% di tutti gli allegati malevoli era costituito da documenti Microsoft Office²⁵.

667% di aumento delle truffe di phishing in un 1 solo mese durante la pandemia di COVID-196.

30% dei messaggi di phishing è stato consegnato di lunedì 29.

32,5% di tutte le e-mail utilizzava la parola chiave «pagamento» nell'oggetto del messaggio.

*statistiche del Threat Landscape – 2020 dell'ENISA e riportati da CISCO

Sitografia

<https://www.enisa.europa.eu>, Agenzia Europea per la cibersicurezza

<https://clunit.it>, Clunit – Associazione Italiana per la Sicurezza Informatica

<https://www.microsoft.com/it-it/security/business/security-intelligence-report>, Microsoft Digital Defense Report

5 Scopriamo cos'è lo spear phishing e come utilizzare il social engineering per colpire le vittime, Panda Security, <https://www.pandasecurity.com/it/mediacenter/panda-security/spear-phishing-come-difendersi/>



Giornalisti in crisi, non la domanda di informazione Di Massimiliano Nespola*

Abstract: La sfida attuale: ideare una strategia di lungo periodo per contrastare la diffusione di notizie false. Grazie agli algoritmi, il lavoro di newsmaking si velocizza e ciò consente di concentrarsi sul giornalismo di qualità.

*Giornalista pubblicista

Il giornalismo è morto, evviva il giornalismo!

Ecco come potremmo iniziare un saggio di approfondimento – o anche una tesi di laurea – sullo scenario attuale della professione. Sarebbe interessante e provocatorio, ma comunque, rimarrebbe un titolo in qualche modo già sentito. Gli studiosi di comunicazione conoscono il cuore del problema: ogni volta che si verifica una trasformazione, spesso tecnologica, o legata ai gusti del pubblico e della società, oppure a fronte di un mutamento culturale, si ha la sensazione che la categoria giornalistica stia per scomparire. Eppure, in realtà ciò non accade.

Il ruolo di mediazione rappresentato dagli “storici del presente” che scrivono sulla sabbia, è in continua evoluzione ed è soggetto a crisi ricorrenti. Tuttavia, a fronte di eventi quali quelli dell’ultimo mese, si avverte ancora forte – e come potrebbe essere il contrario? – la presenza dei professionisti dell’informazione nella nostra società. Ce ne accorgiamo soprattutto al livello relativo all’interpretazione della realtà.

Un ulteriore ambito attualmente posto sotto i riflettori degli studiosi è quello del rapporto tra il giornalismo e l’intelligenza artificiale: quali mutamenti sono all’orizzonte? Senz dubbio, c’è ragione di ritenere che possano informatizzarsi alcuni processi. Questo fatto richiama alla mente il luddismo dell’epoca industriale, perché potrebbe mettere in discussione la necessità di ricorrere a personale in carne e ossa per la produzione delle notizie di agenzia, o comunque una riduzione di unità assunte in tale settore dell’informazione. Si tratta di una trasformazione che avrà comunque dei limiti: l’attività umana di contatto con le fonti e di interrelazione con il pubblico, sapendo ciò che esso si aspetta, non è facilmente sostituibile da un automatismo¹. La visione della realtà e soprattutto



1. Immagine tratta da:

<https://www.ilsaltodellaquaglia.com/2020/12/14/lincubo-fake-news-che-preoccupa-il-mondo/>

la capacità di analisi può anzi uscirne rafforzata: se si liberano risorse destinate alla produzione di contenuti “standard”, si afferma maggiormente il ruolo del giornalista interprete attivo e consapevole dei fatti. Per trovare risposte alla crisi della mediazione giornalistica, un’attività simile ha delle potenzialità di successo, purché e nella misura in cui riesca a trovare sintonia con il pubblico che ha poco tempo a disposizione, ma che comunque ha bisogno di sapere. Le coordinate del mondo, infatti, senza giornali, sarebbero più sfocate, soprattutto considerato che nell’attuale periodo storico non è facile orientarsi: oggi, infatti, il mondo viene rappresentato attraverso migliaia di sfumature di grigio. Se si può attribuire una responsabilità alla categoria, forse è proprio questa: nella dimensione contemporanea, di una presenza consolidata di Internet, quale strumento di “Intelligenza artificiale per il giornalismo: ultime frontiere e limiti irriducibili”, cfr: <https://www.agendadigitale.eu/cultura-digitale/intelligenza-artificiale-per-il-giornalismo-ultime-frontiere-e-limiti-irriducibili/>.

1. Sull’argomento, è stato pubblicato recentemente da “Agenda Digitale” un interessante spunto,

informazione, attraverso cui però possono anche trionfare fake news abilmente costruite, magari diffuse da qualche leader politico tramite i propri canali, emerge più forte di prima la necessità di recuperare il senso. I giornalisti dovrebbero colmare questo vuoto, in cui oggi emerge forte la dimensione tecnologica, algoritmica della comunicazione. Molto è stato fatto, ma la strada da percorrere è ancora lunga, perché il problema che si palesa agli studiosi è quello di comprendere i meccanismi che scattano nel pubblico bersaglio della disinformazione. Il principale ostacolo sembra rappresentato dalla presenza di soggetti interessati a diffondere in società degli schemi interpretativi differenti da quelli riconosciuti dalla maggioranza della comunità scientifica. Rispetto ai dati, è noto infatti che essi non parlano da soli, ma attraverso le modalità di esposizione sui media e facendo riferimento agli obiettivi che ci si prefigge. Ecco quindi che si pongono, in relazione ad internet, alcuni interrogativi: se i numeri si sostituiscono ai fatti e alle persone, quale futuro aspetta loro? Su quale piano porre il reale rispetto al virtuale?

Alcune possibili risposte: i giornali e i giornalisti hanno ancora oggi il compito di contribuire a cercare le verità nascoste. Occupandosi di cronaca o di mafie, di futuro dell'Europa o di politica, il quadro della realtà appare dai contorni non ben delineati. Rispetto ad una potenziale ricerca all'infinito, si ha una responsabilità della categoria: quella di intervenire attivamente, con il pensiero critico quale strumento di ricerca di prove e di adeguata documentazione, rispetto ad un'agenda che spesso è dettata dagli interessi predominanti in società.

I giornalisti hanno il compito di esercitare la mediazione ad un livello alto e di aiutare i cittadini a trovare risposte. Ciò richiede ancora oggi fatica e impegno, dimodoché la loro fiducia non si affievolisca. Nelle istituzioni e nelle strade, nei palazzi e nelle periferie, ovunque sia necessario, il compito del giornalista rimane quello di informare e di documentare ciò che più conta: la verità dei fatti ed una loro ricostruzione chiara e corretta, per i lettori. La rivoluzione digitale degli ultimi decenni non è avvenuta senza lacerazioni e perdite. L'analisi dei dati Audipress (per una lettura approfondita, si rinvia al relativo sito) racconta di un'Italia che già leggeva meno di altri Paesi e in cui si legge di meno rispetto al 2014: i lettori dei quotidiani sono passati, nel complesso, da 40.168.000, a fine 2014, a 29.497.000,

a inizi 2021. Dov'è il lettore? Attraverso quali mezzi e canali si informa? Con quale probabilità di essere informato con trasparenza? Sono domande in costante evoluzione, a cui bisognerà continuare a rispondere.