

## L'indispensabile road-book

per rendere sempre  
più digitale  
e competitiva  
la tua impresa



IN QUESTO NUMERO

## 2023

### un anno di "transizione"

**Crimine e web:** the dark side of the Metaverso

**Facebook e Instagram a pagamento**

**Whistleblowing:**

cos'è, come funziona, perché occorre stare attenti

## L'EDITORIALE

A cura di **Alessio Angioli**

2023

un anno di "transizione"

2023 è al termine: è arrivato il momento di domandarsi a che punto sia la Trasformazione Digitale e che impatto abbia avuto su imprese e pubbliche amministrazioni, ma anche sui cittadini.

### Ma cos'è la Trasformazione Digitale?

È un complesso processo che riguarda tutti i settori, dalla **Finanza** al **Retail** e alla **Logistica**, attraverso un **cambiamento organizzativo in continua evoluzione** che poggia le proprie basi sulle costanti innovazioni digitali e comprende tecnologie come la **Realtà Aumentata**, l'**Internet of Things**, i **Big Data** e il **Cloud Computing**. Sono moltissimi gli aspetti su cui un'azienda dovrebbe lavorare per introdurre e accogliere il processo di Digital Transformation.

Se non altro, per non restare dietro la concorrenza.

### Lo scenario italiano

Nonostante la crescita, l'Italia appare in ritardo rispetto a paesi con economie analoghe come la Francia, la Spagna e la Germania. Secondo il rapporto DESI, è ancora in fondo alla classifica ed è piuttosto debole soprattutto nel settore del Capitale Umano, che tiene conto di competenze digitali e specializzazione ICT.



### I cambiamenti in corso

- **HR - Human Resource** e **Smart Working** sono due segmenti diventati ancora più strategici. Lo **Smart Working**, in particolare, è diventato **determinante** nelle **grandi aziende**, mentre si fa più fatica nella P.A. e nelle PMI.
- Molte aziende, sia pur ancora non abbastanza, hanno investito in **digital learning**, grazie anche a nuove tecnologie digitali a supporto dell'apprendimento, la cosiddetta **Educational Technology (Ed Tech)**.
- Nel settore della **Sanità**, è stata introdotta estesamente la **Telemedicina**, soprattutto in relazione alla pandemia, mentre la **P.A.** ha spinto sui sistemi di Identità Digitale per l'accesso ai servizi online.
- Nel settore **Agrifood** si sta affermando il modello dell'**Agricoltura 4.0**, che ha permesso di affrontare in modo intelligente i costi di produzione e le risorse disponibili, ad esempio, attraverso l'irrigazione di precisione.
- Il settore del Turismo, in pieno ritorno, è trainato dall'**eCommerce** dell'ospitalità, con un fatturato di **19,4 miliardi di euro**, e dei trasporti, con un movimento di **16,9 miliardi di euro**.
- Nel settore della **Logistica**, aumentano i costi produttivi, ottimizzati da un maggiore numero di progetti di digitalizzazione, la **Logistica 4.0**.
- Nel settore del **Retail**, gli investimenti digitali sono rilevanti e stanno testando territori come il **Metaverso**, l'**Intelligenza Artificiale** e l'**Internet of Things**, offrendo **servizi innovativi** sia in ambito **B2C** sia **B2B**.

### I punti chiave da definire per la Trasformazione Digitale in azienda

#### OBIETTIVI:

individuare le esigenze strategiche, reali e raggiungibili

#### COMPETENZE:

incrementare la comunicazione e la formazione delle HR

#### MODALITÀ:

favorire l'inserimento, lo scambio e la diffusione di idee innovative

#### BUDGET:

individuare e allocare le risorse necessarie in termini di investimenti e asset

#### OPERATIVITÀ:

mettere a disposizione gli strumenti per rendere il più agile possibile il processo di innovazione

#### REPORT:

tenere sotto controllo e performance, valutando la complessità, i vantaggi e gli svantaggi



A cura di  
Marco Cecchi

## CRIMINE & WEB: the dark side of the Metaverso

**D**ove ci sono opportunità tecnologiche c'è business; dove c'è business c'è denaro; e dove c'è denaro, spesso, c'è la criminalità organizzata.

La mafia ha colto al volo le opportunità della trasformazione tecnologica in corso ed è urgente una grande attenzione e l'adozione di strumenti adeguati a fronteggiare le nuove minacce.

Le preoccupazioni che stanno nascendo sono di diversa natura - dall'infiltrazione nell'economia legale al turbamento dell'ordine e della sicurezza pubblica.

Le mafie hanno a disposizione tecnologie e tecnici di altissima specializzazione, con alleanze operative e strategiche radicate, anche tra gruppi diversi e di paesi diversi, e il networking è proprio alla base della criminalità "organizzata" che, infatti, ha oltrepassato i "confini nazionali", costituendo una crescente minaccia per la sicurezza degli Stati, delle loro economie e dei diritti dei cittadini. Di conseguenza si va a inficiare la crescita degli equilibri geopolitici ed economici.

Il mondo imprenditoriale, che muove le economie, è fortemente minacciato, per esempio, dalla pubblicizzazione di merci illegali o dalla richiesta del pizzo sui social network che vanno a colpire il tessuto imprenditoriale più produttivo.

Per contrastare il riciclaggio di denaro e il finanziamento delle organizzazioni malavitose, la DIA (Direzione Investigativa Antimafia) consapevole che le battaglie future saranno combattute nel mondo digitale - internet, dark web, metaverso, criptovalute - evidenzia la necessità di un adeguamento normativo da parte dei paesi Ue ed extra Ue. È necessario utilizzare un linguaggio comune, con strategie e normative condivise per contrastare la malavita.

L'obiettivo delle cyberpolice, della quale DIA fa parte, è di investigare nel mondo delle piattaforme virtuali per "seguire il flusso dei soldi sporchi", cercando di prevenirli, ed essere magari un passo avanti a loro.

**Ma anche le aziende devono fare la loro parte.**

**PER DIFENDERSI** dalle minacce mafiose, le imprese dovrebbero costruirsi tutto intorno un'infrastruttura IT solida, costituita da reti, servizi e prodotti certificati originali, di ultima generazione, nonché di cyber sicurezza. Come quelle fornite dagli esperti di I-Team, perché gli avversari sono davvero forti.

*Info Cyber Security Globalnet*



# FACEBOOK e INSTAGRAM a pagamento

## Rimarrete comunque sui social?

**D**a novembre, alcuni utenti italiani dei due grandi social network congiunti nel **brand Meta** hanno ricevuto la possibilità di passare ad un piano a pagamento.

Nonostante Mark Zuckerberg avesse dichiarato che **Facebook sarebbe stato sempre gratuito**, questa appare oggi solamente una delle possibilità. La mission aziendale era stata cercare di connettere tutto il mondo con un servizio accessibile a tutti.

Il modello business di Meta è dovuto recentemente scendere a patti con i regolamenti europei che puntano a limitare la raccolta dei dati, come la **privacy GDPR**, la concorrenza nei **mercati digitali (DMA)** e nei **servizi digitali (DSA)**.

### COSA STA ACCADENDO

I social network stanno diventando a pagamento attraverso l'adesione ad un **abbonamento in modalità "rollout"**, ovvero graduale. Meta tiene a sottolineare che gli utenti non sono obbligati ad abbonarsi, ma potranno continuare ad utilizzare i social network gratuitamente, con qualche differenza.

Gli utenti che decideranno di passare al **piano a pagamento** (*rispettivamente al costo di 12,99 euro al mese per chi utilizza i social su smartphone e di 8,99 euro per chi si affida al browser su web*) non vedranno le **inserzioni pubblicitarie**; questo perché, dal punto di vista della privacy e della sicurezza dati, le **informazioni personali non saranno più tracciabili** e, quindi, utilizzabili ai fini delle inserzioni commerciali.

### E CHI NON SI ABBONA?

Gli utenti che scelgono di **utilizzare gratuitamente Facebook e Instagram** saranno sottoposti a **inserzioni personalizzate**, saranno attori passivi che, nel nostro gergo, chiamiamo **profilati**. Sarà una libera scelta, ma forse non troppo consapevole dei vantaggi e degli svantaggi.

Infatti, l'introduzione dei nuovi abbonamenti ha suscitato molte reazioni ma non tutti gli utenti hanno appunto compreso che chi decida di abbonarsi valuti l'opportunità di eliminare le pubblicità e di proteggere la propria privacy.

Così come molti utenti sono convinti che l'abbonamento sarà reso obbligatorio per tutti. Non è nei piani di Meta ad oggi è **facoltativo**. È bene chiedersi se questa novità creerà anche disparità tra gli utenti paganti e non, per esempio rendendo più sicura l'utenza premium e più vulnerabile quella free. Lo scopriremo nei prossimi mesi.



### E VOI?

Vi abbonate tutelando ufficialmente la vostra privacy  
o preferite lasciare i vostri dati in cambio di un social network gratuito?



# Whistleblowing: cos'è, come funziona, perché occorre stare attenti

**Il** termine riguarda la segnalazione di comportamenti "scorretti" o persino "illegali" in aziende o anche nella PA. Per essere chiari, quando un dipendente scopre una frode, un abuso, la violazione di leggi o regolamenti, una forma di corruzione, è tenuto a segnalare l'irregolarità alla propria azienda che, a sua volta, dovrà adottare misure correttive per evitare ulteriori danni, anche in ottica di pratiche migliorative. Chi segnala è chiamato whistleblower e deve essere tutelato, protetto per non temere ritorsioni discriminatorie o licenziamenti ingiusti.

### LA DIRETTIVA EUROPEA

Il 30 marzo 2023 è entrato in vigore il decreto legislativo 24/2023 che consiste nell'introduzione di una piattaforma informatica sicura che protegga la riservatezza dell'identità e i dati del whistleblower. Entro il 15 luglio le imprese con almeno 250 dipendenti dovranno adottare le regole del decreto; il 17 dicembre 2023 è la scadenza ultima per le imprese che hanno tra i 50 e i 249 dipendenti.

### LE SANZIONI

I responsabili delle violazioni accertate possono incorrere in:

- **sanzioni da 10.000 a 50.000 euro**, la cui applicazione è demandata all'ANAC per i casi di ritorsioni commesse, segnalazioni ostacolate o violazione degli obblighi di riservatezza.
- **sanzioni da 500 a 2.500 euro**, per il segnalante che incorre nei reati di diffamazione o di calunnia o per i medesimi reati commessi con la denuncia all'autorità giudiziaria o contabile.



## La nuova piattaforma **WHISTLEBLOWING** di I-TEAM per imprese e PA

I-TEAM propone la nuova soluzione dedicata al ricevimento e alla gestione delle segnalazioni degli illeciti inviati dai dipendenti, specifica per il delicato contesto della trasparenza e del contrasto alla corruzione.

- **Configurazione personalizzata:** in base al contesto aziendale e alle modalità di gestione delle segnalazioni
- **Riservatezza delle segnalazioni:** impostazioni che rispettano gli obblighi di riservatezza del segnalante in ogni fase di gestione, separando il contenuto della segnalazione dall'identità del segnalante
- **Comunicazione con il segnalante:** comunicazione tra segnalante e gestore della segnalazione senza rivelarne l'identità
- **Conformità normativa garantita:** supporto tecnico e software costantemente aggiornati rispetto all'evolversi del quadro normativo e tecnologico,
- **Assistenza tecnica continuativa:** nessun rischio di obsolescenza, comprensivo di costi per l'aggiornamento
- **Software flessibile:** la piattaforma I-TEAM è utilizzabile da qualsiasi dispositivo

### Che altro dire... il tempo stringe, chiamate I-TEAM!

E, occhio: comportiamoci tutti bene!

# I·TEAM

Cinque società che si sono unite per dare forma a un grande progetto: aiutare le imprese a crescere nella digitalizzazione e nella rivoluzione digitale, per avere performance sempre più efficaci ed efficienti, all'altezza dei grandi cambiamenti dell'economia e della società contemporanea.

 Allyou.srl

 EGO  
communication

 GlobalNet  
Servizi di Telecomunicazioni per la tua Azienda

 OMEGASISTEMI  
Soluzioni Informatiche Professionali

 NETWORK  
PRIVACY



 PANTAREI INFORMATICA  
La tecnologia resa semplice

[WWW.I-TEAM.TECH](http://WWW.I-TEAM.TECH)

Via Benedetto Dei 64 • 50127 FIRENZE • Numero Verde 800-199760 • [info@i-team.tech](mailto:info@i-team.tech)