

NOVEMBRE 2020



IL CAFFÈ DIGITALE

LA TRASFORMAZIONE DIGITALE

Le applicazioni guidano
la trasformazione
digitale di Danone

BANCHE E FINTECH

Come affrontare la
trasformazione digitale e
prepararsi al «New Normal»

QUESTO MESE ABBIAMO FATTO COLAZIONE CON...

Duccio MEDINI

Head of Data Science
and Digital Innovation,
GSK Vaccines

SMART WORKING

Dallo smart working
al lavoro di qualità

IL DIGITALE IN AIUTO DI MODA, LUSO E DESIGN

Sommario

L'EDITORIALE

Il digitale in aiuto di moda, lusso e design.....	2
Emilio Mango	

LA VISIONE DEI LEADER

La strategia dell'Unione Europea per la Cybersecurity.....	4
Diego Ferrara	

NUMERI E MERCATI

Investire nella digitalizzazione del Paese per aumentarne la produttività e la crescita economica.....	8
Carmen Camarca	

FOCUS PA

Infrastrutture digitali per la PA, qual è la direzione?.....	11
Elena Vaciago	

LA TRASFORMAZIONE DIGITALE

Le applicazioni guidano la trasformazione digitale di Danone.....	13
Roberto Bonino	

BANCHE E FINTECH

Come affrontare la trasformazione digitale e prepararsi al «New Normal».....	15
Carmen Camarca	

Open banking, pagamenti digitali e reengineering dei processi: la banca cambia forma.....	17
Carmen Camarca	

CYBERSEC E DINTORNI

Il rischio cyber richiede nel mondo finanziario una risposta di sistema.....	19
Elena Vaciago	

DIRITTO ICT IN PILLOLE

Piano ispettivo del Garante Privacy: quali sono i principali destinatari.....	21
Valentina Frediani	

SMART WORKING

Dallo smart working al lavoro di qualità: come riprogettare l'organizzazione e il lavoro.....	23
Elena Vaciago	

VOCI DAL MERCATO

Lavorare iper-connessi: come farlo?.....	25
Elena Vaciago	



QUESTO MESE ABBIAMO FATTO COLAZIONE CON...



Duccio MEDINI
Head of Data Science and Digital Innovation, GSK Vaccines





L'EDITORIALE

IL DIGITALE IN AIUTO DI MODA, LUSO E DESIGN

Emilio Mango | Direttore, Technopolis

Con il lockdown si moltiplicano le best practice volte a conservare la relazione con i clienti e ad arricchire la customer experience. Le nuove tecnologie sono protagoniste di questa accelerazione verso la trasformazione digitale. Se ne parlerà nel corso di un evento in streaming organizzato da The Innovation Group e Jakala il 10 dicembre.

Con un fatturato di 80 miliardi di euro e quasi 500mila addetti, il settore della moda rappresenta il 12,5% dell'industria manifatturiera italiana in termini di occupati.

L'ultima stima di Confindustria Moda prefigura una perdita, per il settore del fashion, di 29 miliardi di euro (meno 29,7% rispetto al 2019) a causa delle conseguenze del Covid-19; sono valori leggermente migliori rispetto alle stime precedenti ma comunque impressionanti. In generale, i comparti della moda, lusso e design, di solito piuttosto resilienti alle crisi economiche, sembrano questa volta risentire più di altri della prolungata incertezza dovuta alla pandemia.

Questa sta facendo sentire i suoi effetti su più fronti: la crisi del mercato interno e delle esportazioni dovuta ai lockdown attuati in tutto il mondo, la recessione economica ma anche i cambiamenti nelle abitudini di consumo (in primis meno occasioni di socialità).

Ancora una volta, nel senso che è già successo per altri comparti, il digitale sembra però venire in soccorso non solo del settore moda ma più in generale del lifestyle, che comprende quindi anche lusso, design, arredamento.

"Venendo meno il business in presenza", dice Marco Di Dio Roccazzella, General Manager di Jakala, "abbiamo in questi mesi assistito a un'accelerazione del potenziamento dei canali digitali.

D'altronde, il cliente oggi si informa ancora di più attraverso l'online e molte fasi del processo di acquisto che prima venivano realizzate in presenza vengono invece svolte, più o meno efficacemente, a distanza".

Le aziende, quindi, investono sul digitale in modo che le tecnologie possano favorire il processo di conversione e di

“

In questi mesi molti convegni si sono trasformati in show virtuali, permettendo da una parte una discreta esperienza utente nella fase di acquisizione delle informazioni, dall'altra la possibilità di creare o mantenere una relazione con i brand espositori

”

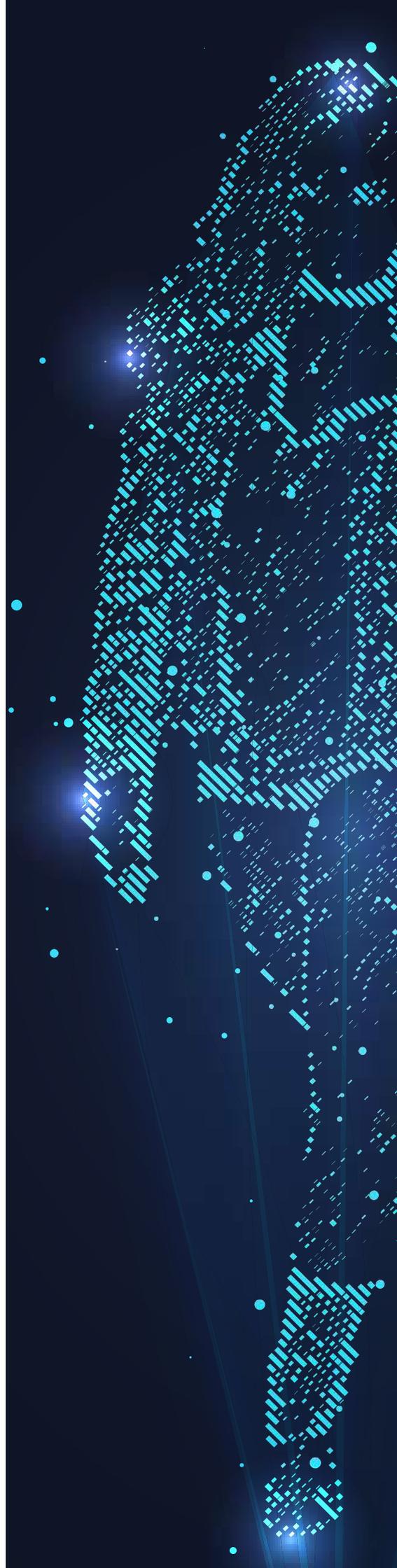
acquisto, con o senza l'ultima tappa in negozio. Parliamo di disponibilità di immagini e informazioni sul prodotto ma anche, ad esempio, del processo di scelta della taglia. "Le nuove tecnologie", prosegue Di Dio Roccazzella, "consentono di mantenere una buona customer experience anche a distanza, sia in negozio sia online: schermi digitali che permettono un dialogo con il sales assistant o anche di provare virtualmente gli abiti e sistemi che in videochiamata abilitano il contatto con l'addetto alle vendite".

In questi mesi, poi, molti convegni e fiere si sono trasformati in show virtuali, permettendo da una parte una discreta esperienza utente nella fase di acquisizione delle informazioni, dall'altra la possibilità di creare o mantenere una relazione con i brand espositori e, perché no, gli altri partecipanti all'evento.

"C'è poi una trasformazione digitale in atto anche nel backoffice", conclude Di Dio Roccazzella, "perché tutte le aziende stanno spingendo per mettere a fattor comune del business il Crm, l'unico modo per far sì che le piattaforme e-commerce e social possano veramente instaurare un dialogo profittevole con il cliente anche a negozi chiusi".

Infine, non dobbiamo trascurare il tema della post vendita.

Con il lockdown il tema della cura del cliente e del prodotto nelle altre fasi del ciclo di vita commerciale è diventato ancora più centrale: una fonte di best practice che, una volta finita la pandemia, possono risultare utili anche in tempi di "nuova normalità" a tutti i brand, compresi quelli meglio posizionati.



LA VISIONE DEI LEADER

La strategia dell'Unione Europea per la Cybersecurity



Diego Ferrara
Cybersecurity Policy Officer, Commissione Europea

Intervento effettuato durante la Web Conference del 10/09 "L'ESPERIENZA DELLA CYBERSECURITY IN TEMPI DIFFICILI: COSA ABBIAMO IMPARATO" appuntamento del Digital Italy Program 2020 #LaVisioneDeiLeader

Negli ultimi anni la Commissione Europea ha prestato grande attenzione all'ambito della cybersecurity: nel 2013 si è partiti con una strategia cybersecurity europea, che è stata rivista successivamente e ha portato al primo atto legislativo a livello europeo in materia di cybersecurity, la Direttiva sulla sicurezza delle reti e dei sistemi informativi (Direttiva Nis) entrata in vigore nel 2016. Il regolatore europeo ha quindi proseguito nel 2017 con il Cybersecurity Package e con il Cybersecurity Act (entrato in vigore nel 2019), con cui ha introdotto il sistema di certificazione. Gli anni a venire ci vedranno impegnati su diversi fronti, con la prevista revisione della Direttiva Nis, l'implementazione del Cybersecurity Act e della certificazione, la finalizzazione di un'altra proposta legislativa riguardante il Centro di Competenza Europeo per la cybersecurity (ancora in fase negoziale, si punta a concludere entro l'anno).

Per quanto riguarda la revisione della prima direttiva Nis, questa mira a promuovere e rafforzare la capacità di resilienza e di cybersecurity attraverso gli Stati membri dell'Unione Europea, ad assicurare quindi che ci sia un livello omogeneo di resilienza in tutta l'Unione. La Commissione ha deciso di anticipare la revisione della direttiva per perfezionare il funzionamento di alcuni punti chiave della

LA COMMISSIONE
HA DECISO DI
ANTICIPARE LA
REVISIONE DELLA
DIRETTIVA NIS PER
PERFEZIONARE IL
FUNZIONAMENTO DI
ALCUNI PUNTI
CHIAVE DELLA
DIRETTIVA

Direttiva come ad esempio il processo di identificazione da parte degli Stati membri degli operatori di servizi essenziali.

Il processo di revisione include varie fasi: una valutazione di come gli Stati membri abbiano identificato gli operatori di servizi essenziali sul territorio; visite in tutti gli Stati membri per avere una risposta sui punti di forza e sui punti deboli della direttiva; una consultazione aperta a tutti gli stakeholders per contribuire al processo di revisione; il processo formale di valutazione della direttiva e l'analisi di impatto sulla futura direttiva rivista, per passare infine al processo di policy making con il coinvolgimento di Parlamento e Consiglio.

Dal punto di vista invece dei vantaggi prodotti dalla Nis, la maggiore capacità degli Stati membri nel rispondere agli attacchi cyber e anche una migliore cooperazione a livello operativo attraverso la rete europea dei centri di risposta a livello nazionale. Anche durante la pandemia, questi meccanismi sono stati utili per facilitare lo scambio di informazioni sugli incidenti cyber che toccavano ai vari Stati membri. Inoltre, la direttiva ha mirato a promuovere per la prima volta una cultura di gestione del rischio nei vari Stati membri e ad aumentare il livello di sicurezza delle reti e dei sistemi d'informazione a livello europeo.

Le nuove iniziative dell'Unione Europea mirano a rafforzare la cybersecurity dei prodotti, dei servizi e dei processi, grazie al Cybersecurity Act, o a promuovere l'attività di ricerca e sviluppo di soluzioni cyber. Per quanto riguarda il Cybersecurity Act, la novità è l'introduzione

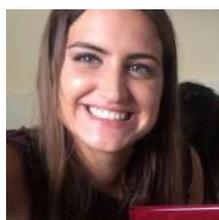


di un quadro di certificazione volontaria a livello europeo, con norme che facilitano il set up di vari schemi parametrati per prodotti, servizi e processi cyber. Inoltre, è stato rinnovato anche il processo che porta all'emergenza dei vari schemi, partendo da un Union Rolling Work Programme con le priorità per quanto riguarda la certificazione di prodotti, servizi e processi. Questo programma è ora in fase di redazione, con due gruppi di lavoro, lo Stakeholder cybersecurity certification group e l'European cybersecurity certification group, il primo con stakeholders privati (daranno un input dal punto di vista degli operatori di servizi critici e dei produttori, dei laboratori per esempio), mentre il secondo gruppo di lavoro è composto dalle autorità nazionali dei paesi membri. Una volta stilato questo programma, la Commissione potrà richiedere all'ENISA di redigere una prima bozza di schema. Infine, un terzo aspetto è come saranno gestiti i futuri fondi di ricerca dell'Unione Europea in materia di cybersecurity; a questo riguardo, la proposta è quella di creare un centro di competenza per gestire i fondi per la cybersecurity derivanti dai nuovi programmi di ricerca e innovazione dell'Unione, il futuro programma Horizon Europe e il Digital Europe Program.. Il centro Europeo, che gestirà un network di centri di competenza nazionali, dovrà contare anche sulla partecipazione degli stakeholders privati (qualora decidessero di far parte di questa comunità). In ultimo, un accenno anche al Fondo CEF – Connecting European Facilities, attualmente è aperta una call per la cybersecurity che offre la possibilità di inviare una proposta entro fine novembre.



QUESTO MESE ABBIAMO FATTO COLAZIONE CON

L'impatto della data analysis nell'industria farmaceutica



Intervista di **Ezio Viola e Carmen Camarca** a
**Duccio Medini, Head of Data Science and Digital Innovation,
GSK Vaccines R&D**

In vista dell'“AI & Data Forum Live 2020” di The Innovation Group, che si terrà il prossimo 17 novembre, abbiamo intervistato Duccio Medini, Head of Data Science and Digital Innovation, GSK Vaccines R&D, che ci ha parlato di come la trasformazione digitale stia impattando sull'industria farmaceutica e di cosa comporti realizzare attività e progetti di data sharing in un settore in cui i dati trattati sono di estrema sensibilità. Riportiamo di seguito la prima parte dell'intervista che proseguirà nel prossimo numero della newsletter e si soffermerà in modo particolare sull'utilizzo dell'Intelligenza Artificiale e Analytics nell'ambito della vaccinologia e quali implicazioni ciò comporta in un periodo caratterizzato da una forte attenzione ai vaccini e alle cure sperimentali per combattere il Covid-19.

All'interno dell'industria farmaceutica, quali sono oggi gli aspetti più significativi del processo di trasformazione digitale che il settore sta vivendo? In particolare, quali implicazioni si rilevano in relazione all'utilizzo del dato e alla sua capacità di creare valore?

In modo simile a quanto sta avvenendo in altri verticali, advanced analytics e intelligenza

artificiale stanno trasformando l'intera value-chain dell'industria farmaceutica. Un'area molto attiva in questo momento è la progressiva integrazione dei dati che vengono generati nelle prove cliniche randomizzate con i dati che vengono definiti di Real World per sostituire le evidenze empiriche generate con i clinical trial con Real-World Evidence.



I dati di Real World sono molteplici, includono dati di registri elettronici di ospedali, delle società di assicurazione che si occupano di salute privata o delle strutture di salute pubblica, nonché dati di salute generati direttamente dall'individuo attraverso device, applicazioni ed ecosistemi (che sempre più i giganti tecnologici entrati nel settore stanno potenziando). Ciò si accompagna ad una serie di implicazioni, oltre che di carattere scientifico e tecnologico (di data integration, accesso al dato ed estrazione

di informazioni), anche in termini di privacy (trattandosi di dati relativi alla salute dell'individuo) e di valore associato al dato, ovvero di ownership ed informazioni che si possono estrarre.

Essendo il settore farmaceutico una delle industrie più regolate in assoluto, un ruolo chiave è svolto dal regolatore che negli ultimi cinque anni si è mostrato sempre più favorevole verso l'apertura

di questo tipo di dati come sorgente di evidenza e decisione, un fenomeno che comporta molte opportunità per il futuro.

A cosa è dovuta questa forte spinta del regolatore? Nasce da una maggiore consapevolezza dell'importanza di queste tematiche considerata l'attuale situazione sanitaria oppure vi erano già in precedenza delle sollecitazioni?

La regolamentazione della ricerca farmaceutica è nata dopo la seconda guerra mondiale, in seguito alle terribili sperimentazioni eugenetiche compiute da medici nazisti, favorite dall'assenza di regolazione. Molta dell'attuale legislazione è stata sviluppata nel secolo scorso per impedire che chiunque – industria farmaceutica, medici o governi – potesse nuovamente violare principi etici fondamentali, e per garantire che la ricerca che coinvolge esseri umani sia sempre solida e generi risultati credibili. Dopo un periodo di assestamento, in cui si è cominciata a percepire l'esigenza di adattare tali misure pur non volendo rinunciare alle garanzie di una forte regolazione, si è arrivati in questi ultimi anni alla consapevolezza che la tecnologia di cui oggi si dispone può permettere di rendere la stretta regolamentare più flessibile ed efficiente, senza però perdere il controllo e rinunciare alla sicurezza. È questo cambiamento culturale che sta guidando l'apertura che oggi caratterizza il settore verso l'utilizzo delle nuove tecnologie.

Oltre alla necessità, si avverte anche la volontà di fare data sharing?

L'interesse a fare data sharing per lo sviluppo di farmaci è dibattuto da oltre 10 anni. Si possono rilevare alcune iniziative in cui diverse aziende farmaceutiche stanno collaborando per comprendere cosa condividere con i competitor generando un vantaggio comune ma non una violazione della sana competizione. Ad esempio, Gsk è stata la prima azienda a decidere autonomamente, nel 2013, di rendere disponibili i propri dati sul clinical trial a chiunque lo richieda affidando la valutazione della ragione per cui viene richiesto accesso ai dati ad un trust esterno. L'esempio è stato seguito da altre aziende ed oggi si è evoluto in una piattaforma chiamata "Clinical Study Data Request", supportata da più di 15 sponsors, che permette a chiunque abbia una motivazione adeguata di chiedere l'accesso ai dati di quasi 3000 trial clinici.

Tuttavia, l'impressione che si avverte è che, nonostante la volontà di fondo e interessanti case studies (in cui si avverte la sempre più forte convinzione sul vantaggio che un pieno data sharing comporterebbe per tutta la comunità e i player del settore), manchi un ecosistema del dato di salute in cui diversi player possano, in modo trusted, affidare i dati all'utilizzo fair da parte della comunità.



Si tratta di un fenomeno che neanche la pandemia può accelerare?

La mancanza di questo ecosistema è una delle cause principali della parzialità e della limitata efficacia della risposta con cui tutti i governi stanno reagendo a questa seconda ondata pandemica di COVID-19. Se si fosse stati in possesso di un ecosistema in cui i dati raccolti potevano essere condivisi attraverso standards interoperabili e con le giuste garanzie, probabilmente questa fase di recrudescenza della pandemia sarebbe stata gestita in maniera differente.

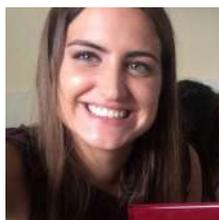
A cosa si deve la mancanza di questo ecosistema?

All'incrocio di tre elementi.

1. Un aspetto culturale. L'industria farmaceutica ha radici profonde, tutti i principali player del settore hanno più di 100 anni di storia, non è facile indirizzare tali attori in un'ottica di digitalizzazione e di open data e verso un approccio di ecosistema.
2. La giusta cautela che tutti gli attori (e in particolare il regolatore) mostrano verso le problematiche di privacy. Il grande valore del dato è legato alla sua individualità più che alle percentuali statistiche e di massa. Da questo punto di vista si rileva un forte gap tecnologico che non riguarda la creazione dell'ecosistema (le tecnologie necessarie per creare un back-end tecnologico sono già disponibili) ma la garanzia di un controllo adeguato e dinamico su problematiche di privacy.
3. Questione di massa critica. Uno dei modi possibili per lanciare un ecosistema è che un player veda il business e lo crei. Tuttavia, quello del software per la ricerca farmaceutica è un mercato più piccolo di altri, e il rischio associato all'investimento tecnologico tradizionale finora ha generato più tentativi di stabilire monopoli chiusi che di favorire ecosistemi aperti.

NUMERI E MERCATI

Investire nella digitalizzazione del Paese per aumentarne la produttività e la crescita economica



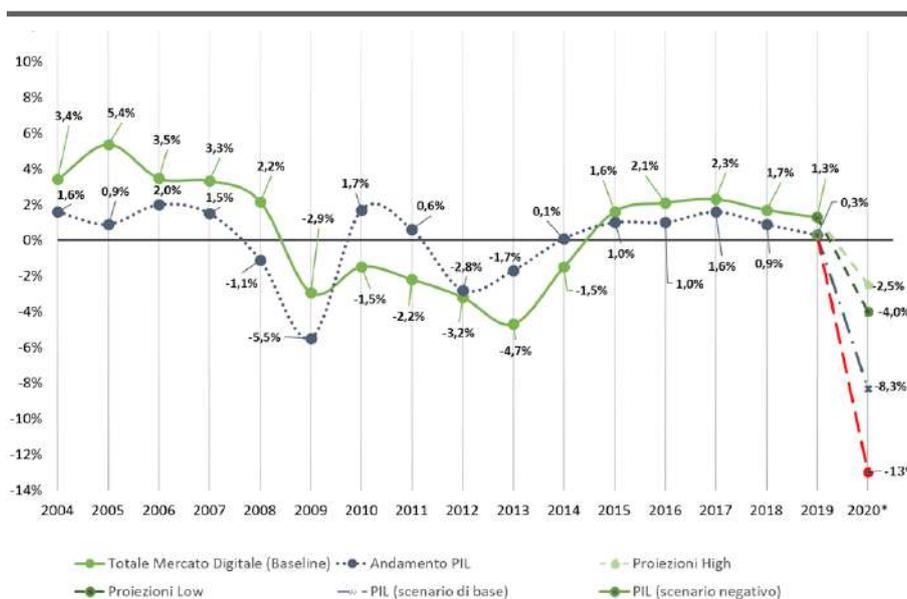
Carmen Camarca
Analyst, The Innovation Group

Nella sua consueta attività di analisi sull'andamento del mercato digitale, The Innovation Group ha rilevato come la relazione tra il PIL e il mercato digitale,

salvo rare eccezioni, sia sempre stata di carattere ciclico, tale per cui i tassi di crescita del mercato digitale tendono ad aumentare al crescere del PIL e a diminuire quando questo flette. Quest'anno, pur rilevando una decrescita per le due variabili considerate, è possibile

osservare un trend differente che indurrebbe a riflettere sulla possibilità che il digitale possa effettivamente svolgere un ruolo anticiclico rispetto al PIL. Secondo, infatti, le ultime previsioni di The Innovation Group, a fronte di

una flessione del PIL compresa tra il -13% e il -8,3%, il mercato digitale dovrebbe limitare le proprie perdite al -2,5% (nello scenario positivo) o al -4% (nello scenario negativo).



Fonte: TIG

Tali trend sono stati discussi lo scorso 20 ottobre nell'ambito del Digital Italy Web Summit 2020 durante la sessione plenaria "Lo scenario del mercato digitale nell'anno della Pandemia", in cui si è cercato di comprendere se la forte attenzione dedicata al digitale in questo

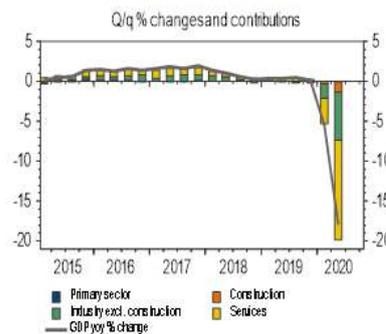
periodo sia il risultato di una reazione all'emergenza oppure rappresenti una tendenza strutturale dell'economia italiana, facendo della pandemia la "killer application" da tempo attesa nel mercato per far decollare il digitale.

Nel suo intervento introduttivo alla sessione, e volto a rappresentare lo scenario macroeconomico, Gregorio De Felice, Chief Economist, Intesa Sanpaolo, ha confermato la performance positiva del mercato ICT e digitale, considerato uno degli ambiti meno colpiti dall'impatto della pandemia, a differenza di settori quali il turismo, la cultura e i trasporti. Inoltre, la digitalizzazione, la tecnologia e il tracking, oltre alla maggiore preparazione dei governi e della popolazione, riusciranno ad evitare un nuovo lockdown produttivo e generalizzato che potrebbe causare conseguenze ben più drammatiche di quelle rilevate in seguito all'applicazione delle prime misure restrittive.

Dagli studi di Intesa Sanpaolo emerge, altresì, una forte crescita, nel terzo trimestre del 2020, della produzione industriale, per cui si può parlare di una ripresa a V: si consideri che il settore manifatturiero, lo scorso agosto, ha raggiunto i livelli pre-Covid, registrando, nel terzo trimestre dell'anno, un aumento del 30% sul precedente e confermando la resilienza del sistema produttivo italiano nonché la sua forte capacità di ripresa nonostante il blocco dello scorso marzo. Come mostra il grafico seguente, l'industria manifatturiera italiana si presenta, in ambito europeo, come quella con il più alto tasso di crescita nel periodo post lockdown.

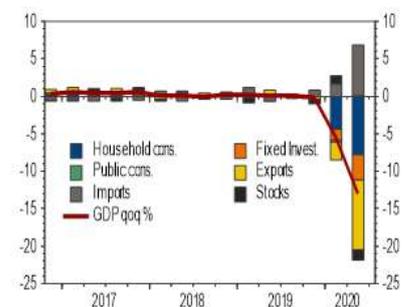
quest'anno, una decrescita del PIL pari al 9,5% con un rimbalzo del 6,5% per l'anno prossimo, con, tuttavia, dei forti rischi a ribasso. In uno scenario favorevole, il biennio 2020-2021 si concluderà con una perdita del PIL pari al 3,6%, un gap che l'Italia, con i suoi storici ritmi di crescita (pari a circa lo 0,6% annuo), recupererà intorno al 2026/27. Un simile scenario, rende ancora più necessario realizzare riforme strutturali e interpretare al meglio i nuovi mega trend dell'ambiente e del digitale per permettere un forte incremento della produttività di tutto il sistema Paese.

L'apporto più negativo al valore aggiunto viene dai servizi



Fonte: Istat, elaborazioni Intesa Sanpaolo

Dal lato della domanda, i contributi più negativi vengono da consumi ed export



Fonte: Istat, elaborazioni Intesa Sanpaolo

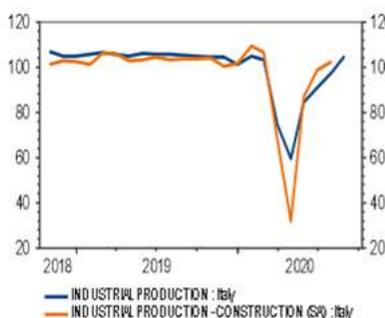
Quali, dunque, le politiche industriali più efficaci da promuovere?

A parlarne è stato Marco Gay, Presidente, Anitec-Assinform e Confindustria Piemonte, secondo cui i principali ambiti di intervento sono sette, quattro relativi al lato della domanda e tre dell'offerta.

Con riferimento alla domanda, il focus deve essere su:

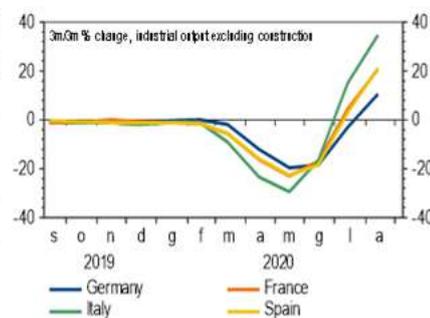
- Imprese e cittadini, concentrandosi sul rafforzamento dei fondi (crediti di imposta, ammortamento, voucher) che incentivano la domanda di tecnologie abilitanti (AI, analytics, cloud).
- Amministrazioni Pubbliche e infrastrutture, con un'attenzione particolare alla digitalizzazione dei servizi erogati dalla Pubblica Amministrazione.

Produzione industriale sopra i livelli pre Covid



Source: Istat, Intesa Sanpaolo calculations

Ripresa più sostenuta che in altri Paesi UE



Source: Eurostat, Intesa Sanpaolo calculations

A fronte della ripresa dell'industria manifatturiera vanno, tuttavia, rilevati i forti impatti che il lockdown ha avuto sul segmento dei servizi per cui, fatta eccezione per alcuni settori (quale appunto quello ICT e digitale), si rileva una grave recessione.

In tale contesto, Intesa Sanpaolo prevede, per

- Scuola, dotando gli edifici scolastici di un'infrastruttura digitale e promuovendo investimenti significativi nell'ambito della didattica a distanza.
- Sanità, potenziando, soprattutto in questo periodo, le attività di contact tracing e l'interoperabilità tra le diverse strutture.

Per quanto riguarda l'offerta, invece, gli ambiti sono:

- R&S. Allo stato attuale, in Italia l'86% degli investimenti in ricerca e innovazione è supportato dalle imprese private, a fronte di un solo 14% di finanziamenti pubblici. Ciò comporta la necessità di incrementare l'impegno pubblico, soprattutto tramite l'assunzione di ricercatori ed esperti.
- Startup innovative, che rappresentano un trasformatore naturale di innovazione. In Italia, sebbene si rilevi una crescita del fenomeno si avverte ancora la necessità di supportarne lo sviluppo con specifici piani esecutivi.
- Competenze ICT. Investire su questo asset consente al Paese di trasformarsi su tre ambiti: qualificazione professionale (gli studenti devono possedere competenze ICT

a prescindere dal proprio percorso di studi), riqualificazione professionale (la trasformazione tecnologica ha bisogno di dotarsi di nuove competenze anche da parte di chi già possiede un lavoro), l'accrescimento e il continuo rinnovamento delle competenze (la tecnologia cambia e bisogna seguirne l'evoluzione).

Il Paese necessita che tali riforme vengano realizzate quanto prima e il periodo storico che si sta vivendo con l'arrivo delle numerose risorse previste dal Recovery Fund rappresentano una condizione favorevole perché ciò accada, ma il policy maker sarà in grado di applicare le misure necessarie per assicurare che il sistema economico e produttivo del Paese possa beneficiare del fondamentale ruolo che il digitale può svolgere per esso?



FOCUS PA

Infrastrutture digitali per la PA, qual è la direzione?



Elena Vaciago

Associate Research Manager, The Innovation Group

L'emergenza Covid19 ha portato le Pubbliche Amministrazioni italiane a confrontarsi con l'urgenza di digitalizzare le attività, eliminando i blocchi che avevano ritardato questa evoluzione in passato. Il lockdown ha fatto emergere in maniera ancora più evidente le criticità strutturali del Paese, mettendo in crisi le infrastrutture IT di alcuni enti del settore pubblico. Abbiamo avuto varie esperienze negative, come negli ultimi giorni per il blocco del portale buonomobilità.it del Ministero dell'ambiente per erogare il bonus biciclette. Un evento che ha ricordato il caos di aprile con le richieste del bonus sul sito INPS, andato in tilt per un eccesso di domanda. La situazione sta mettendo in luce la necessità di accelerare la trasformazione in chiave digitale, sempre più richiesta – da cittadini e imprese – a chi eroga servizi pubblici. La ripresa dovrà essere il momento per creare infrastrutture resilienti che siano alla base di un più ampio percorso di innovazione e digitalizzazione dell'intero Paese.

Il tanto auspicato passaggio al cloud della PA promette maggiore agilità delle infrastrutture, integrazioni con intelligenza artificiale, interoperabilità e controllo sui dati, efficientamento e sicurezza.

Come modernizzare le infrastrutture e aggiornare le competenze per erogare servizi digitali pubblici efficienti, con un occhio alla razionalizzazione delle risorse e a una più ampia semplificazione dei rapporti con i cittadini? Come accelerare nei percorsi di digitalizzazione, abilitando lavoro agile ed efficienza operativa, adottando un modello operativo per il cloud comprensivo di automazione, governo e analisi, sia per contenere i costi, sia per

elevare le prestazioni ed incrementare la resilienza operativa?

Il tanto auspicato passaggio al cloud della PA promette maggiore agilità delle infrastrutture, integrazioni con intelligenza artificiale, interoperabilità e controllo sui dati, efficientamento e sicurezza. L'utilizzo di tutte queste tecnologie – integrate tra loro

– dovrebbe permettere alle istituzioni di effettuare un salto in avanti nell'erogazione di servizi qualitativamente superiori.

Questi temi sono stati al centro dei lavori del Digital Italy Summit 2020, principale evento

italiano sui temi dell'innovazione a livello Paese, in particolare nella Sessione "Agenda Digitale, Infrastrutture e piattaforme pubbliche: a che punto siamo con l'Execution?" del 21 ottobre 2020. L'incontro è stato l'occasione per fare il punto sull'avanzamento del nuovo piano Triennale per l'informatica nella Pubblica Amministrazione (2020-2022) pubblicato lo scorso agosto da Agid. Come ha detto Francesco Paorici, Direttore Generale di Agid intervenendo al Digital Italy Summit 2020: "Quest'anno abbiamo disegnato il Piano Triennale Agid con maggiore attenzione all'Execution. Abbiamo previsto indicazioni operative e concrete su asset strategici, come servizi, dati, piattaforme, infrastrutture, interoperabilità e sicurezza. Il coinvolgimento attivo delle PA e dei territori. Un approccio orientato alla misurazione dei risultati, in cooperazione con le PA, con indicatori di risultato per obiettivi strategici e un monitoraggio continuo".

Sistemi e servizi affidabili richiedono infrastrutture funzionanti e sicure. Per questo, gli ambiti di intervento del Piano Triennale sono:

- Dal punto di vista della sicurezza informatica, aumentare la consapevolezza del rischio cyber nella PA e il livello di sicurezza informatica dei servizi digitali;
- Dal punto di vista dei Dati, puntare a condivisione e riutilizzo di dati aperti tra la PA e da cittadini e imprese, oltre che aumentare la qualità dei dati e le politiche di valorizzazione del patrimonio informativo pubblico;
- Per servizi e inclusività: migliorare la qualità, l'esperienza d'uso e l'accessibilità dei servizi pubblici digitali.

Un tema critico come noto è quello delle Infrastrutture utilizzate dalle PA. La recente rilevazione di Agid (il Censimento del Patrimonio ICT della PA) ha evidenziato come molte infrastrutture risultino prive dei requisiti di sicurezza e di affidabilità necessari e siano carenti sotto il profilo strutturale e organizzativo. Dei 1.252 data center coinvolti nel censimento, in base ai parametri di classificazione, solo 35 risultano idonei ad essere utilizzati come Polo Strategico

Nazionale (PSN), (e di questi, solo 27 classificati nel gruppo A, ovvero con carenze strutturali o organizzative considerate minori) mentre ben 1.190 dovrebbero essere dismessi quanto prima.

Dove con Polo Strategico Nazionale delle Infrastrutture Digitali (PSN) si intende l'insieme delle infrastrutture digitali localizzate all'interno del territorio nazionale, ad alta disponibilità, che potrebbero garantire alle PA elevati livelli di sicurezza, affidabilità ed efficienza energetica.

Ci stiamo avvicinando quindi a definire i requisiti del futuro "Cloud della PA"? Anche di recente il Ministro Paola Pisano avrebbe fatto riferimento per questo progetto a un'infrastruttura ad elevato livello di sicurezza (con uno o più poli) su cui convogliare i dati che i CED delle amministrazioni locali, e anche di alcune centrali con livelli non sufficienti di sicurezza, ricorrendo a partnership pubblico-privato sul modello di quelle adottate in UK. "Occorre un cloud per i dati della Pubblica Amministrazione che non comprometta le autonomie delle sue varie componenti. Questa operazione dovrà avvalersi di fondi, parte dei quali per permettere a singole amministrazioni di rendere digitali i propri servizi" ha detto il Ministro Pisano, sottolineando anche l'impegno del Governo a promuovere un protocollo cloud UE, come quello del progetto Gaia-X, sempre per il recupero della sovranità sui dati (nel frattempo, chi già si propone per Gaia-X sono molte grandi organizzazioni del settore privato, come Leonardo, Enel, Aruba, Retelit, Confindustria digitale, Cy4Gate).

Sul percorso di razionalizzazione e maturazione a livello di infrastrutture digitali per le PA, valgono alcune best practice, tra tutte il ruolo di Sogei. "La nostra Execution parte da un forte ingaggio dei dipendenti verso i clienti, piattaforme abilitanti e un'infrastruttura centrale. Ci consideriamo una società aperta, orientata a creatività e contaminazione – ha detto Andrea Quacivi, AD di Sogei, intervenendo al Digital Italy Summit 2020. La tecnologia non è l'unico fattore abilitante, bisogna investire anche sulla cultura dei dipendenti, su digital skill e sulla capacità

manageriale. L'obiettivo deve essere quello di realizzare piattaforme e prodotti a servizio del Paese".

Insomma, emerge da tutti i contributi una nuova direzione verso la concretezza e la governance efficace, un tentativo di arrivare finalmente a reali risultati comuni, in un percorso di trasformazione graduale e consapevole delle infrastrutture IT nella PA italiana.

Il censimento del patrimonio ICT - Risultati classificazione del Data Center

I risultati della classificazione definitiva dei Data Center al termine della fase 3 è il seguente:

35
Candidabili*

27
GRUPPO A

1190
GRUPPO B

*Per «Candidabili» si intendono le infrastrutture candidabili all'utilizzo da parte di un PSN che soddisfano tutti i requisiti riportati nella colonna «Candidabilità all'uso da PSN» (allegato A della Circolare 1/2019).

Fonte: Censimento ICT della PA, Agid, 2019

LA TRASFORMAZIONE DIGITALE

Le applicazioni guidano la trasformazione digitale di Danone



Intervista di **Roberto Bonino** a
Alberto Biasuzzi, IS Domain Leader Operations Sud Europa, Danone

A colloquio con Alberto Biasuzzi, IS Domain Leader Operations Sud Europa di Danone, per capire quali sviluppi stiano assecondando l'innovazione dell'azienda.

Mutuando la definizione dall'iniziale boom del mondo mobile, molti studi hanno parlato di quella che stiamo vivendo come l'epoca della application economy.

Lo sviluppo del software, che sia totalmente gestito all'interno delle aziende oppure affidato in tutto o in parte a specialisti esterni, riveste un ruolo determinante per l'evoluzione del business delle aziende.

Nel corso della storia informatica, ogni passaggio evolutivo ha seguito un percorso naturale, segnando un miglioramento progressivo rispetto a ciò che c'era prima e generando significativi aumenti di produttività.

Oggi siamo di fronte a un nuovo step, legato all'affermazione di metodologie Agile, concetti come DevOps e logiche come quelle dei container e dei microservizi, che rendono possibili lo sviluppo e le integrazioni continue ovvero la risposta più naturale alle esigenze di velocità e innovazione connesse ai processi di trasformazione digitale.

Per capire come queste dinamiche si innestano in una grande multinazionale come Danone, ci siamo

intrattenuti con Alberto Biasuzzi, IS Domain Leader Operations Sud Europa.

Quali sono oggi le aree applicative che meglio definiscono i processi di trasformazione digitale in atto nella vostra azienda?

A livello italiano non disponiamo di siti produttivi, quindi gli ambiti più significativi di innovazione sono collegati alle relazioni con clienti, consumatori e partner strategici.

L'emergenza sanitaria di questo 2020 ha poi generato un impatto rilevante anche sui processi interni, in particolar modo sulla comunicazione e le modalità di lavoro e collaborazione, ma anche su processi volti ad aumentare l'efficienza e ridurre i passaggi rispetto ai modelli tradizionali.

Se spostiamo il raggio d'azione al Sud Europa, stiamo accelerando molto nella digitalizzazione dei siti produttivi, rendendo concreto il paradigma Industria 4.0.

Importante è anche l'area della collaborazione con i partner logistici, destinata a diventare ancora più digitale di quanto già non fosse fino a poco tempo fa, con l'obiettivo dell'eliminazione totale della carta e dell'aumento della tracciabilità dei prodotti, a vantaggio anche dei consumatori.

Quali sono le priorità che guidano i processi di sviluppo?

Negli ultimi mesi è cresciuta notevolmente l'attenzione verso la sicurezza, mentre in un

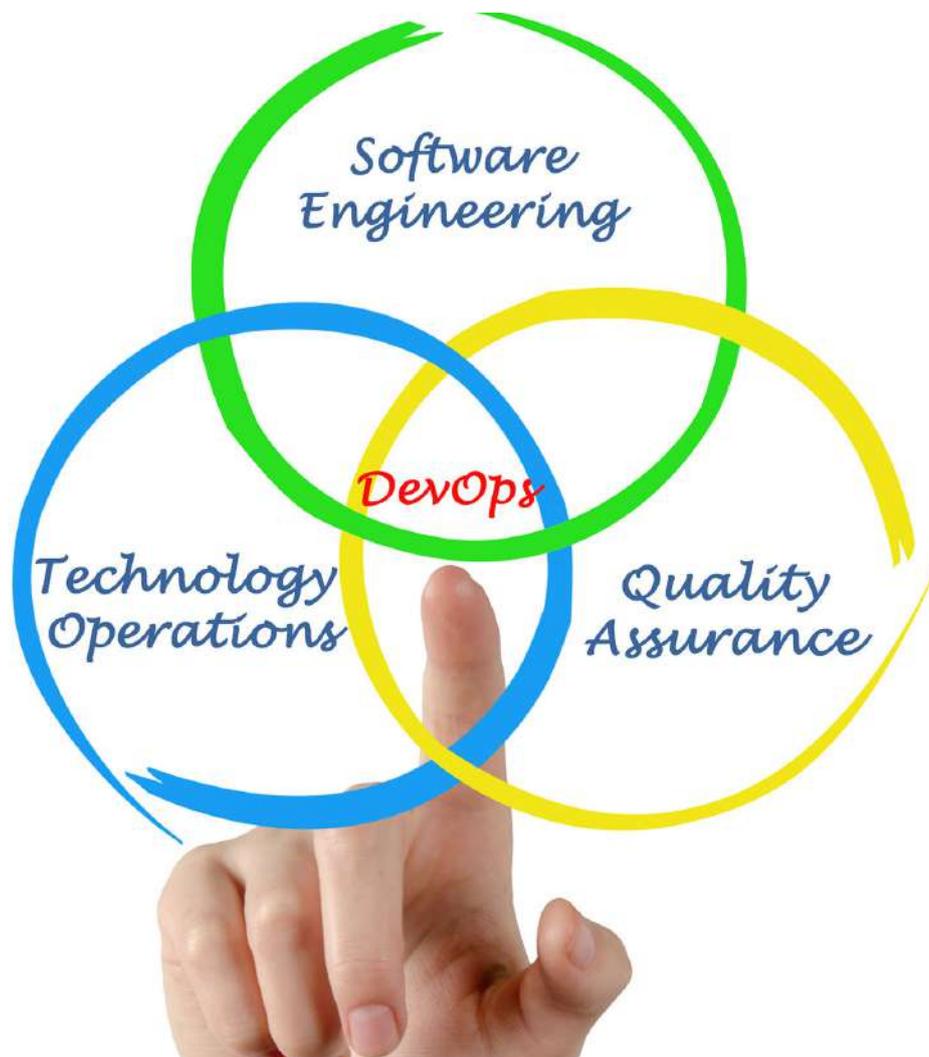
passato ancora recente la priorità numero uno era il time-to-market.

Per diverso tempo, ci siamo preoccupati soprattutto di essere veloci e subito corretti, quindi senza fare errori nell'esecuzione dei progetti.

Oggi, invece, ci stiamo occupando di più di sicurezza nei confronti dei clienti, dei consumatori e dei partner, ovviamente in combinazione con una velocità di rilascio sempre fondamentale.

Come sfruttate modelli come DevOps a supporto della trasformazione in corso?

Nel mondo del marketing, il peso del digitale è ormai fondamentale in diverse direzioni.



NEGLI ULTIMI MESI

È CRESCIUTA

L'ATTENZIONE VERSO

LA SICUREZZA, MENTRE

IN UN PASSATO

ANCORA RECENTE LA

PRIORITÀ NUMERO

UNO ERA IL

TIME-TO-MARKET

Qui l'adozione del modello DevOps è già un dato di fatto.

Ci sono laboratori, all'interno del gruppo, che hanno già consegnato applicazioni in uso anche in altri ambiti, come per esempio la semplificazione delle attività di customer service, per avere a disposizione cruscotti utili per fare sintesi e azioni più mirate.

Stiamo lavorando anche nel mondo delle applicazioni commerciali, per esempio nella raccolta ordini o sul punto vendita, con trasmissione di immagini dei prodotti e qualche sperimentazione di realtà aumentata.

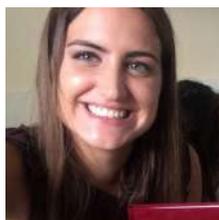
Quali saranno gli sviluppi a breve e medio termine?

Sicuramente sono attese evoluzioni sul fronte dell'e-commerce, mentre sul fronte più operativo prevediamo di intervenire sulla logistica, in particolare nel percorso fabbrica-magazzino e in quello magazzino-consumatore.

In prospettiva, sfruttando anche nuove tecnologie ora in fase di studio, vorremmo arrivare al punto di servire il nostro cliente nel momento in cui lo chiede e dove lo chiede.

BANCHE E FINTECH

Come affrontare la trasformazione digitale e prepararsi al «New Normal»



Carmen Camarca
Analyst, The Innovation Group

Se, da un lato, il Covid-19 ha provocato, nell'industria bancaria, l'accelerazione di fenomeni in precedenza timidamente in atto, dall'altro ha reso necessarie per gli operatori delle trasformazioni radicali. Tra queste si rilevano, in modo particolare, fenomeni quali:

- il forte declino dell'utilizzo del cash,
- l'accelerazione nell'utilizzo dell'online banking (in modo particolare del mobile),
- l'utilizzo del web per la comunicazione tra dipendenti e con i clienti,
- il social distancing negli uffici e nelle filiali,
- l'estensione del Remote/Smart Working (in alcuni casi definito "Working Aware", soprattutto nella seconda fase dell'emergenza) e il conseguente potenziamento di strumenti e soluzioni tecnologiche innovative (ampliamento dell'utilizzo del cloud, ricorso a software di collaboration) per garantire la continuità operativa.

Tali tematiche sono state affrontate lo scorso 9 ottobre, in occasione del Banking Summit Live 2020. Nel dettaglio dalle testimonianze dei Chief Operating Officer di alcuni dei principali istituti bancari del Paese è emerso che, tra gli impatti della pandemia sulle attività di operation della banca, è stata rilevata un'importante riorganizzazione del modo di lavorare, potenziando in maniera massiccia lo smart working (in alcuni casi già avviato) che ha coinvolto anche il modello di funzionamento delle filiali e le modalità di interazione con il cliente.

Rimane comunque la consapevolezza che tutte le attività non possono essere svolte da remoto e che permangono alcuni ambiti in cui la relazione fisica continuerà ad avere un valore, rendendo, dunque, necessario identificare quali attività possono essere svolte in presenza e quali in modalità agile.

Tali cambiamenti non hanno, tuttavia, impattato sulla produttività del personale: in particolare, dall'esperienza di Danilo Augugliaro, COO, Ing è emerso come la remotizzazione del lavoro abbia comportato un aumento della disciplina, nonostante siano state registrate alcune perdite di produttività legate ad una comunicazione meno fluida rispetto a quella face to face.

La situazione di contingenza ha, inoltre, comportato sfide sotto diversi aspetti, in particolare dal punto di vista tecnologico ed organizzativo. Dalla testimonianza di Vittorio Calvanico, COO, Banca Monte Dei Paschi di Siena è, infatti, stato rilevato come la tecnologia non fosse in realtà pronta ad affrontare cambiamenti di una portata così vasta come quelli vissuti. Ad ogni modo, nella fase più acuta dell'emergenza, le banche hanno dimostrato una capacità di reazione improvvisa che ha superato le attese: in particolare, è stata rilevata l'estrema rapidità con cui fasce di popolazione di clientela ritenute più difficilmente convertibili si sono adattate al cambiamento. Anche le strutture di legacy hanno dimostrato di poter essere convertite in una realtà diversa.

L'esperienza di Paola Angeletti, COO, Intesa Sanpaolo ha, infine, mostrato come il processo di

trasformazione digitale abbia comportato, oltre che una profonda trasformazione nell'assetto organizzativo interno, anche nel modo di selezionare i migliori talenti. L'esperienza vissuta ha del resto acceso i riflettori sul tema del ricambio generazionale e della necessità di introdurre, all'interno degli istituti bancari, nuove competenze: aree come il risk management e la compliance necessitano costantemente di figure professionali altamente specializzate, così come i reparti dell'IT, della cybersecurity e l'area digital.

Oltre alla continua ricerca di nuove figure professionali viene avvertito il bisogno di sviluppare specifici programmi di reskilling per i dipendenti (alcuni di questi sono stati promossi per la figura del gestore o del consulente da remoto).

In questo contesto come ricostruire, dunque, il «New Normal»?

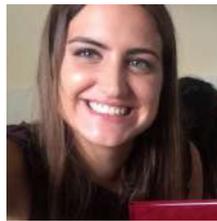
Dalle esperienze riportate emerge la necessità di realizzare processi più agili altamente digitalizzati, mantenendo tuttavia la consapevolezza che inevitabilmente alcune attività continueranno ad essere svolte da remoto. Bisognerà, inoltre, promuovere all'interno degli assetti organizzativi ambienti flessibili, meno strutturati di quelli che caratterizzano le banche "tradizionali" ed essere resilienti.

In vista di tali cambiamenti, la tecnologia e lo strumento digitale, già in questa fase protagonisti continueranno a svolgere un ruolo sempre più rilevante: in particolare si prevede un ulteriore potenziamento degli strumenti di collaborazione da remoto, oltre che una forte attenzione a tutto ciò che consente la creazione di ambienti agile e che permette di accedere, fruire ed estrarre valore dai dati.



BANCHE E FINTECH

Open banking, pagamenti digitali e reengineering dei processi: la banca cambia forma



Carmen Camarca
Analyst, The Innovation Group

Secondo un'indagine ABI Lab^[1], per le banche le principali aree di investimento ICT sono lo sviluppo di piattaforme API/ introduzione di modelli di Open Banking e la modernizzazione dei propri sistemi core, fenomeni accelerati negli ultimi mesi ma che già negli anni precedenti avevano modificato in maniera significativa l'industria bancaria e finanziaria, intervenendo su business model, modalità di erogazione dei servizi, processi interni e, soprattutto, sulla relazione con il cliente.

Le due tematiche sono state oggetto di specifiche sessioni parallele lo scorso 8 ottobre in occasione del "Banking Summit Live 2020" in cui sono state riportate le testimonianze di alcune delle principali

realità bancarie del Paese (Intesa Sanpaolo, ING, Crédit Agricole Italia). Di seguito vengono riportate le principali evidenze emerse dalla discussione. Il paradigma dell'Open Banking rappresenta una "tempesta perfetta", generata, da un lato, dalla compliance e dall'adeguamento alla normativa PSD2 e, dall'altro, dalla possibilità di attivare, grazie a partnership e ad aperture a servizi terzi, nuovi business model.

Infatti, la consapevolezza della banca di aver bisogno di un'alleanza digitale apre alla possibilità di sviluppare servizi forniti da altri partner, di introdurre innovazione dalle fintech

e di ampliare le partnership con chi opera all'interno dell'ecosistema, abilitando nuovi use case su clienti sia consumatori sia esercenti.



Fonte: TIG

Per le banche nuove opportunità si creano anche in relazione alla forte accelerazione dei pagamenti digitali, la cui crescita ha coinvolto sia i consumatori sia gli esercenti, un trend spinto dal Piano Cashless del Governo^[2] e dal forte ricorso alle modalità di acquisto online ed e-commerce rilevato negli ultimi mesi.

Il fenomeno rappresenta un fattore chiave anche in un'ottica di miglioramento della customer experience, permettendo di abilitare nuovi servizi attorno al cliente, nonché di conoscerlo meglio e di essere più vicino ai suoi needs.

Il modello piattaforma, infatti, su cui si basa il successo di aziende appartenenti ad industry differenti (si pensi, ad esempio, all'entertainment o al food delivery) abitua il cliente ad esperienze sempre più personalizzate, aumentandone le aspettative e la forte accelerazione dei pagamenti digitali può rappresentare una chiave rilevante per proliferare meglio il cliente e abilitare nuovi servizi.

Perché ciò accada, tuttavia, sono necessari ingenti volumi di dati, oltre che un'adeguata data strategy così da poter fornire con successo alla propria clientela servizi a valore aggiunto.

Perché ciò accada, oltre ad ingenti volumi di dati, si rende necessario anche possedere fondamenta digitali forti, ridurre i silo e intervenire sul legacy system.

Infine, una forte attenzione alla cybersecurity è un elemento trasversale all'interno di tutti questi layer.

L'importanza di digitalizzare le attività di operation e back office per snellire i processi e migliorare la CX. L'emergenza ha reso ancora più evidente per le banche l'importanza di digitalizzare i processi di operation e back office e di modernizzare i sistemi di legacy utilizzando tecnologie avanzate (RPA, AI, BPM, ecc..).

Come, infatti, è emerso durante l'evento la modernizzazione dei processi è stato uno dei principali ambiti in cui le banche intervenute hanno dichiarato di aver investito e sviluppato progetti innovativi.

Attività di questo tipo si sono rese necessarie sia perché avessero un miglior impatto sull'intera organizzazione (soprattutto in un periodo in cui la maggior parte della forza lavoro operava da remoto) sia per comprendere la user experience degli operatori di filiale e il customer journey dei

propri clienti. In particolare, la reingenerizzazione e dematerializzazione dei processi hanno permesso di snellire le attività di back office, determinando la capacità di rispondere al cliente in maniera estremamente più reattiva ed efficace, aspetto che ha assunto ancora più rilevanza nell'ultimo periodo, in cui è emersa, da parte del cliente, una fortissima esigenza di care.

In tale contesto, la principale sfida è il mantenimento di un'architettura agile in cloud e lo sviluppo di strategie data driven basate sulla capacità di intercettare dati di qualità ed estrarne intelligenza in real time.

È stato, infine, rilevato un forte ricorso a soluzioni di Intelligenza Artificiale per migliorare l'esperienza utente dei clienti (al riguardo si citano casi d'uso quali lo sviluppo di chatbot sia testuali sia vocali per fornire supporto alla clientela) e nell'ambito della fraud detection, area in cui sempre più l'intervento umano deve

essere supportato da un sistema, in modo particolare nell'individuazione dei segnali falsi positivi (sempre più frequenti).

Per le banche l'utilizzo in maniera molto estesa delle applicazioni di Intelligenza Artificiale richiede innanzitutto un'adeguata gestione dei dati, l'individuazione dei KPI e la

condivisione delle informazioni da parte dei team di data science, oltre che determinate conoscenze e skill, requisito fondamentale per lo sviluppo di qualsiasi attività it driven volta a generare valore in termini di ottimizzazione e miglioramento dei processi.

La reingenerizzazione e dematerializzazione dei processi hanno permesso di snellire le attività di back office, determinando la capacità di rispondere al cliente in maniera estremamente più reattiva ed efficace.

[1] "Rilevazione sulle priorità ICT delle banche italiane", marzo 2019, 22 banche/gruppi bancari e 4 outsourcer interbancari

[2] Il piano prevede un premio di 3 mila euro per le prime 100mila persone che nell'arco di 6 mesi, dal primo dicembre 2020 (quando dovrebbe partire) fino a fine maggio 2021 avranno effettuato il maggior numero di transazioni con carte e altri strumenti di pagamento e va ad aggiungersi al cashback che prevede la restituzione del 10% delle spese sostenute (con rate semestrali) con questo tipo di transazioni per un ammontare massimo di 3 mila euro. Il rimborso viene riconosciuto solo se si effettua un numero minimo di 50 transazioni ogni 6 mesi.

CYBERSEC E DINTORNI

Il rischio cyber richiede nel mondo finanziario una risposta di sistema



Elena Vaciago

Associate Research Manager, The Innovation Group

Nel luglio del 2019, Capital One, operatore finanziario USA specializzato in carte di credito, prestiti e conti di risparmio, è stato colpito da uno dei più gravi incidenti di cybersecurity nella storia delle banche, con perdita di dati personali (compresi i numeri delle carte di credito) per cento milioni di persone. A distanza di un anno, Capital One ha acconsentito a pagare una multa di 80 milioni di dollari, per non aver previsto le corrette misure di sicurezza (nello specifico, i dati erano in un archivio mal configurato in cloud, e a divulgarli è stato un hacker di 33 anni, Paige Thompson, in precedenza dipendente di Amazon).

Perché il settore finanziario è così tanto esposto ai rischi cyber?

Come riporta un Report della società di consulenza Boston Consulting Group, la probabilità di incorrere in problematiche di cybersecurity è molto più alta nel mondo dei servizi finanziari:

“Financial services firms are 300 times as likely as other companies to be targeted by a cyberattack, and dealing with those attacks and their aftermath carries a higher cost for banks and wealth managers than for any other sector.” (BCG Report)

Da un lato il mondo Finance è ovviamente un target attrattivo per una moltitudine di potenziali attori. Dall'altro lato, per sua natura è soggetto a un'ampia esposizione alle minacce provenienti dal mondo digitale, con possibili ricadute sistemiche, come sarà anche discusso nel corso del Workshop Live “Cybersecurity In Financial Services” organizzato da

The Innovation Group nella mattina del prossimo 25 novembre 2020. Le attività finanziarie sono infatti:

- Ampiamente digitalizzate, con una superficie d'attacco molto estesa, un trend che negli ultimi mesi ha subito un'ulteriore accelerazione a causa del remote working e dell'ulteriore digitalizzazione della relazione con il cliente.
- Le transazioni finanziarie avvengono in tempi rapidissimi (quindi sono potenzialmente soggette a una diffusione istantanea di un eventuale contagio).
- Le operazioni e i servizi finanziari sono sempre più aperti (pensiamo agli effetti della PSD2) oltre che interconnesse con terze parti non sufficientemente controllate.
- Il settore è fonte di dati molto attrattivi per il cyber crime.
- Le banche e gli altri attori dipendono moltissimo dal Trust che i loro clienti ripongono nell'istituto, e quindi sono potenzialmente molto soggette a un eventuale danno di reputazione.
- Sono soggette a una normativa molto ampia e complessa, quindi esposte anche a rischi legati alla conformità.
- Sono esposte a numerosi rischi legati al fattore umano, favoriti da comportamenti errati nella quotidianità lavorativa.

In aggiunta vanno considerati i rischi propri del mondo finanziario, che in alcuni casi sono diventati molto sofisticati: pensiamo ad esempio agli attacchi alla rete SWIFT o alle vulnerabilità delle Fintech.

An attractive target... 45% have suffered economic crime during the survey period compared to only 34% across all other industries.

More than one way to lose... The sector remains a key target for criminals and asset misappropriation is still the primary type of reported economic crime. Cybercrime, bribery and corruption appear to be increasingly common in the sector.

Tone from the top... 1 in 5 internally-perpetrated frauds still involve senior management, though the majority of such fraud tends to be committed by junior staff or middle management.

Delusions of security... Cybercrime risk appears to be increasing – however, risk awareness can differ greatly depending on an individual's role and function.

Where the money's at... Money laundering remains a hot topic in the FS sector, where it is almost five times more likely to occur than in other industries.

Named and shamed... FS organisations fear the fallout of being caught up in money laundering – almost 30% believed that the most severe impact is reputational.

Telling... Whistleblowing mechanisms appear to be more prevalent than before, however doubts remain over their effectiveness.

Underestimating the risk... 1 in 4 FS respondents failed to conduct annual fraud risk assessments. Over half of those who have not conducted any at all during the survey period are unaware of what these assessments involve or fail to see value in them.

Fonte: TIG

Attacchi alla rete SWIFT

Il sistema di messaggistica SWIFT è stato disegnato per realizzare transazioni sicure e veloci tra i diversi operatori finanziari: tuttavia, abbiamo visto negli ultimi 3 anni almeno a una decina di incidenti di sicurezza in cui il sistema è stato aggirato e sfruttato per portare enormi guadagni a bande di cyber criminali. Utilizzando le credenziali SWIFT, gli hacker sono infatti stati in grado di convogliare grandi importi su propri conti bancari prontamente svuotati dopo il colpo. Dopo il famoso colpo alla Banca centrale del Bangladesh del 2016, per 81 milioni di dollari andati persi, ne sono avvenuti molti altri, come quello alla Indias City Union Bank per 2 milioni di dollari nel febbraio 2018, e quello per 6 milioni di dollari a una Banca russa nel 2017, sempre per alcune debolezze del sistema SWIFT (poi risolte).

Vulnerabilità delle Fintech

Grazie al rapido sviluppo tecnologico, le Fintech, startup del settore finanziario, hanno creato nuovi modelli di business, App e processi innovativi per pagamenti peer-to-peer, prestiti online, gestione della finanza personale user friendly, aggiornamenti e alert in real time. Le Fintech mettono i clienti in grado di effettuare molto più velocemente e facilmente operazioni sempre effettuate tramite le Banche, a costi inferiori se non del tutto gratuitamente, con una tecnologia avanzata. Il problema è che, per fare tutto questo, le Fintech hanno spesso posto la sicurezza in secondo piano rispetto allo sviluppo e al time-to-market. Le statistiche sui rischi legati alle Fintech sono spesso molto negative: secondo ImmuniWeb, ad esempio, il 98% delle top 100 startup fintech globali sono vulnerabili alle più comuni forme di attacco cyber (come phishing, attacchi alla sicurezza delle App mobile, ecc). Tra i problemi più frequenti individuati per le Fintech rientrano: pratiche di data security; modelli utilizzati per la condivisione di dati; gestione delle identità digitali dei clienti; vulnerabilità lato cloud e piattaforme web utilizzate.

Il problema è che – quando problematiche come la perdita di dati o le transazioni malevole colpiscono un attore del mondo finanziario – le perdite (per i clienti) possono essere molto elevate. Le Fintech mancano di un corretto controllo dei rischi, presentano un forte ricorso a terze parti (piattaforme, cloud provider) e sono anche spesso esse stesse integrate nelle piattaforme di grandi istituti finanziari, rendendo tutto il sistema quindi potenzialmente molto più fragile.

Prepararsi a un futuro più sicuro per i servizi finanziari

Il mondo della finanza europeo sta cominciando ad aggregarsi per rafforzare le difese con una strategia comune contro il cybercrime. Per farlo la BCE ha

promosso la Cyber Information and Intelligence Sharing Initiative (CIISI-EU) a cui hanno aderito soggetti pubblici e privati. A unire le forze, sotto l'impulso dei partecipanti all'Euro Cyber Resilience Board for pan-European Financial Infrastructures (ECRB) presieduto dalla Bce, sono banche centrali, controparti centrali, depositari centrali, sedi di negoziazione, gestori di sistemi di pagamento, fornitori di servizi tecnologici e di rete e l'Europol. Obiettivo dell'iniziativa è quello di proteggere il sistema finanziario attraverso la prevenzione, il rilevamento tempestivo e la risposta coordinata agli attacchi informatici. Inoltre, sarà facilitata la condivisione di buone prassi per far accrescere la consapevolezza delle infrastrutture finanziarie sulle minacce alla sicurezza informatica. La Banca d'Italia partecipa al CIISI-EU per il suo ruolo di gestore di sistemi di pagamento in ambito nazionale e per l'Eurosistema. A gennaio di quest'anno poi, Banca d'Italia e Consob hanno concordato una strategia comune per rafforzare la sicurezza cibernetica del settore finanziario italiano attraverso specifiche misure rivolte alle infrastrutture finanziarie: sistemi di pagamento, controparti centrali, depositari centrali e sedi di negoziazione dei titoli. Il piano d'azione congiunto riguarda diverse aree di intervento: regolamentazione e supervisione, cooperazione pubblico-privato, formazione e sviluppo di consapevolezza sui rischi cibernetici. In particolare, la Banca d'Italia e la Consob utilizzeranno strumenti di valutazione del rischio cyber, già adottati nell'ambito dell'Eurosistema, come le Cyber Resilience Oversight Expectations for Financial Market Infrastructures (CROE), metodologia per la supervisione del rischio cyber. La Banca d'Italia e la Consob svilupperanno inoltre il TIBER-IT, modello per lo svolgimento di test derivato dal framework europeo di Threat Intelligence-Based Ethical Red Teaming (TIBER-EU), valutandone l'ambito, le modalità e la tempistica di applicazione alle diverse entità finanziarie, secondo un principio di gradualità che tenga conto del livello di preparazione degli operatori.

DIRITTO ICT IN PILLOLE

Piano ispettivo del Garante Privacy: quali sono i principali destinatari



Valentina Frediani
General Manager, Colin & Partners

Pubblicato il piano ispettivo dell’Autorità di Controllo per la protezione dei dati personali, valido sino a fine anno 2020. L’Autorità, periodicamente, stabilisce le priorità di controllo rispetto alle risorse disponibili per poter effettuare l’attività ispettiva di iniziativa.

L’impegno si concretizza in interventi in loco da parte dell’Ufficio – o delegando la Guardia di Finanza – nei luoghi dove si effettuano i trattamenti di dati; dove occorre effettuare rilevazioni comunque utili al medesimo controllo; nei confronti di soggetti non necessariamente individuati sulla base di reclami o segnalazioni (che sono l’altra “origine” dei controlli).

Analizziamo dunque gli ambiti indicati dall’Autorità. Innanzi tutto, dobbiamo premettere che l’attività ispettiva di iniziativa è suddivisa in: “controlli nei confronti di soggetti, pubblici e privati, appartenenti a categorie omogenee sui presupposti di liceità del trattamento e alle

condizioni per il consenso qualora il trattamento sia basato su tale presupposto, sul rispetto dell’obbligo dell’informativa nonché sulla durata della conservazione dei dati” e “accertamenti in riferimento a profili di interesse generale per categorie di interessati”.

Gli accertamenti riguarderanno innanzi tutto il cosiddetto whistleblowing ovvero quei trattamenti di dati personali effettuati mediante l’uso di applicativi per la gestione delle segnalazioni di condotte illecite (si pensi al tema 231). Su questo tema era già intervenuta l’Autorità Garante perché si pone la necessità di porre particolare attenzione alle garanzie a favore degli interessati che, rilasciando informazioni funzionali a eventuali indagini su illeciti, possono dare esposizione del proprio rapporto lavorativo. Ciò ricade sugli strumenti di trattamento, dei quali occorre dimostrare l’analisi del rischio e le misure conseguenziali, ma anche sul processo



organizzativo del flusso dei dati stessi e sulla loro conservazione. Sotto verifica anche la presenza di idonea informazione preventiva verso l'interessato che carica i dati di riferimento.

Destinatari degli accertamenti anche i trattamenti dei dati personali effettuati da intermediari per la fatturazione elettronica. In questo caso si tratterà di effettuare controlli funzionali alla verifica – in particolare – di tematiche connesse alla protezione, in considerazione delle importanti masse dati.

Si rinnova poi l'attenzione, prestata anche nel primo semestre 2020 con provvedimenti ad hoc, verso quelle realtà che gestiscono e registrano le telefonate nell'ambito della prestazione di servizi di call center. Le sempre frequenti segnalazioni al Garante, non fanno che evidenziare come questo ambito non sia sufficientemente gestito in conformità, in particolare laddove sussistano esternalizzazioni "selvagge" che non tengono in considerazione le prescrizioni del GDPR.

Possiamo sicuramente affermare, anche in considerazione degli esiti dei controlli come emersi dalle comunicazioni dell'Autorità, che appaiono piuttosto scarni gli accordi contrattuali e, soprattutto, raramente presenti audit adeguati da parte dei Titolari. Ciò non fa che aumentare il livello di attenzione da parte dell'Autorità.

Inoltre, condizionati dalla pandemia e dal lockdown, sotto la lente anche il settore del Food Delivery in considerazione dei dati dei consumatori sempre più oggetto di raccolta e di potenziale profilazione, oltre che massivamente trattati, che rendono necessaria una tutela effettiva.

Infine, gli accertamenti riguarderanno anche gli enti pubblici (con particolare riferimento ai sistemi di rilascio di certificati anagrafici e di stato civile, attraverso l'accesso ad ANPR) ed il tema, più generico, del data breach.

Su quest'ultimo possiamo osservare come, negli ultimi mesi, il ricorso allo smart working abbia provocato un aumento importante degli attacchi favoriti da utenti evidentemente meno vigili nella gestione della sicurezza una volta fuori dall'ambiente lavorativo.

Dunque, si profilano interventi trasversali che avranno impatto su quelle realtà che operano una gestione massiva di dati. Si tratta spesso di organizzazioni in ambito B2C, senza tralasciare questioni prettamente aziendali come il breach o il whistleblowing.

Ricordiamo che, rispetto all'obbligo di adottare e recepire il GDPR secondo un principio di accountability, tutte le scelte operate dai Titolari devono essere storicizzate e ne deve essere data evidenza durante eventuali controlli.



SMART WORKING

Dallo smart working al lavoro di qualità: come riprogettare l'organizzazione e il lavoro



Elena Vaciago

Associate Research Manager, The Innovation Group

La pandemia ha favorito il ricorso al lavoro a distanza in modo inedito in Italia (e a livello mondiale) sia durante il lockdown sia dopo. Con la ripresa, in molti – lavoratori e datori di lavoro – puntano a mantenerlo avendo verificato con mano i benefici del nuovo paradigma. Ma cosa significa, nel bene e nel male, lavorare iper-connessi? Durante il Tavolo di Lavoro “Smart Working: come sta trasformando il lavoro, le imprese e le organizzazioni pubbliche. Il ruolo della tecnologia”, che si è tenuto nel pomeriggio del 21 ottobre durante il DIGITAL ITALY SUMMIT 2020, è stato dibattuto:

- Quali sono i risultati ottenuti nel settore pubblico e privato con riferimento alla promozione del lavoro agile.
- Quali sono i punti di attenzione perché questo percorso possa beneficiare di ampia adozione e di una corretta impostazione.
- Come riorganizzare processi e ruoli, nel breve e lungo periodo, per beneficiare di quanto oggi realizzabile con la tecnologia.

Con riferimento al primo punto (i risultati ottenuti ad oggi con riferimento a un ripensamento e una trasformazione dei modelli lavorativi), durante la discussione sono emersi molti commenti positivi.

Paolo Sottili, Direttore Generale, Direzione Centrale Organizzazione di Regione Liguria, ha sottolineato ad esempio: “Oggi, dopo mesi di smart working emergenziale, stiamo tornando al regime ordinario, anche se abbiamo in parte modificato la normativa dell’Ente per rendere più flessibile l’utilizzo di tale

modalità di lavoro. Mentre durante l’emergenza avevamo le persone attive in smart working per 4 o 5 giorni alla settimana, e per molte settimane consecutive, ora si torna ad avere una prevalenza del lavoro svolto presso l’ufficio con un massimo di due giornate di lavoro agile alla settimana, fruibili, all’occorrenza, anche in modo continuativo nel mese”.



Come ha poi aggiunto Paolo Sottili, lo smart working emergenziale ha dato una fortissima spinta alla digitalizzazione delle attività e allo sviluppo delle relative competenze. Sono stati avviati nell’ultimo periodo processi che fino all’anno scorso sembravano condannati alla carta; sono partiti processi già informatizzati che altrimenti non sarebbero mai decollati. Nel settore pubblico, una forza lavorativa con età media elevata ha dovuto apprendere in poco tempo a lavorare in modo nuovo: anche questo un risultato importante e inedito.

Attenzione però agli elementi critici nel passaggio a nuovi modelli di lavoro. Da questo punto di vista le osservazioni emerse durante il Tavolo di Lavoro sono state numerose: come ha detto Mario Attubato, Corporate Head of Digital Transformation di Saipem: "Il tema non è tanto tecnologico o digitale in sé. Siamo già da tempo dentro un modo nuovo di lavorare, in un New Normal, ed è fondamentale considerare il tema di formare le persone al nuovo modo di lavorare smart, perché al momento vediamo che non si sono ancora abituate".



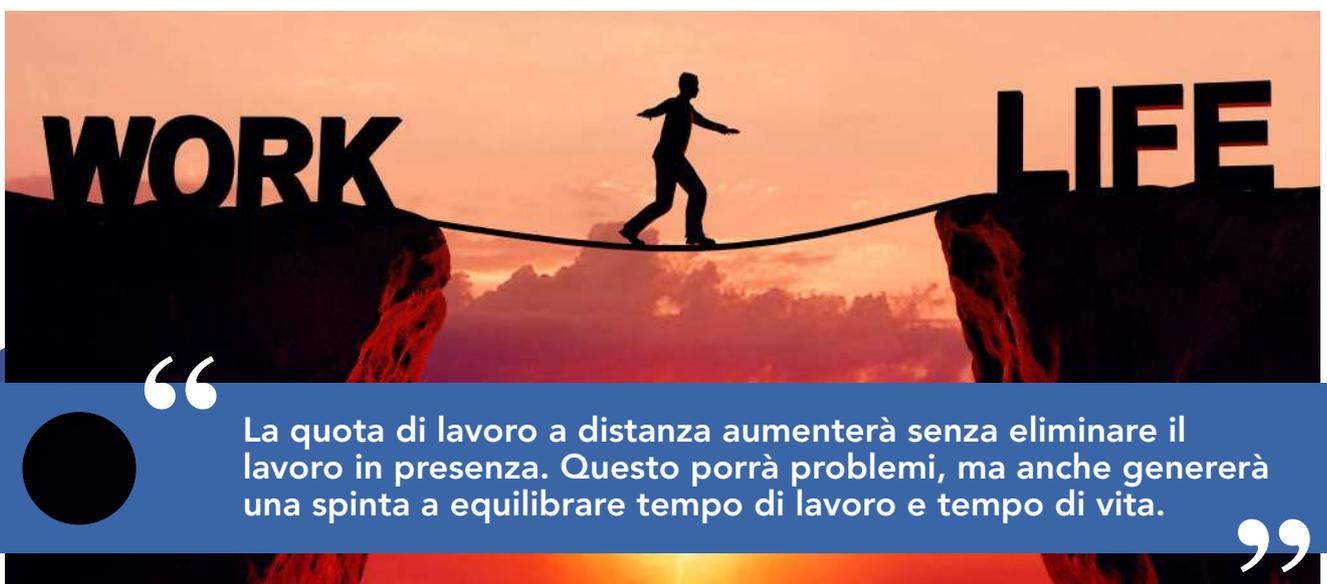
L'impressione che si trae da una convivenza forzata con il lavoro intermediato dalla tecnologia, come è successo quest'anno a livello macroscopico, è che tutto sia più rigido e impersonale, quasi "incastrato" in una pianificazione che pervade ogni momento, lascia poco spazio all'informalità e all'improvvisazione, chiede di rispondere in modo molto veloce a obiettivi che diventano istantanei, richiede nuove capacità per una corretta gestione dei tempi e delle performance personali.

Anche per Silvia Cassano, Responsabile Risorse Umane di ING Italia va bene spingere sul digitale (ING è stata la prima Banca a introdurre in Italia, lo scorso agosto, lo smart working super flessibile, con massima autonomia e responsabilizzazione delle persone) ma bisogna avere grandissima attenzione alle persone, a garantirgli una vita soddisfacente da tutti i punti di vista. Quindi, identificare quali sono i "momenti importanti" in cui è comunque preferibile

essere in ufficio, avere diritto alla disconnessione, avere la possibilità di interagire di frequente con il management e i colleghi, essere informati su come cambiano con lo smart working anche i percorsi di carriera.



Per quanto riguarda infine le sfide che ci aspettano nel futuro, cosa servirà fare prioritariamente e come riorganizzare processi e ruoli, per beneficiare di quanto oggi realizzabile con la tecnologia nel breve e lungo periodo, viene in aiuto la lezione del Professore Federico Butera, Presidente, Fondazione IRSO, sulla rivista HBR Italia ("Dallo smart working al lavoro ubiquo di qualità: un'opportunità per cambiare il lavoro e le organizzazioni") dove innanzi tutto si distingue tra misure pubbliche (ricerca, un nuovo assetto normativo, investimenti e incentivi fiscali) e misure adottate dalle singole organizzazioni (infrastrutture, mindset, riprogettazione di processi e uffici, relazioni industriali). Poi, come conclude Federico Butera: "La quota di lavoro a distanza aumenterà senza eliminare il lavoro in presenza. Questo porrà problemi, ma anche genererà una spinta a equilibrare tempo di lavoro e tempo di vita. Andrà riprogettata la domesticità del lavoro insieme a un impulso a migliorare l'organizzazione della vita familiare e a valorizzare il tempo libero, dando maggior valore allo stare in casa come stiamo imparando forzatamente durante il lockdown di questi giorni. Non sarà facile ma si può e si dovrà fare anche dopo, indipendentemente dal numero di giorni alla settimana in cui si lavorerà da casa".



“

La quota di lavoro a distanza aumenterà senza eliminare il lavoro in presenza. Questo porrà problemi, ma anche genererà una spinta a equilibrare tempo di lavoro e tempo di vita.

”

VOCI DAL MERCATO

Lavorare iper-connessi: come farlo?



Intervista di Elena Vaciago a
**Paolo Sottili, Direttore Generale, Direzione Centrale Organizzazione
di Regione Liguria**

Cosa significa, nel bene e nel male, lavorare iper-connessi? Ne parliamo in questa intervista con Paolo Sottili, Direttore Generale, Direzione Centrale Organizzazione di Regione Liguria, che su questi temi è intervenuto lo scorso 21 ottobre nel corso del Tavolo di Lavoro "Smart Working: come sta trasformando il lavoro, le imprese e le organizzazioni pubbliche. Il ruolo della tecnologia" nell'ambito del DIGITAL ITALY SUMMIT 2020.

Con la fine dello smart working "emergenziale", organizzazioni del settore pubblico e privato stanno puntando a mantenere quanto imparato durante la fase emergenziale, in termini di maggiore produttività e più ampia accettazione del lavoro svolto da remoto. Qual è la situazione in Regione Liguria?

Oggi, dopo mesi di smart working emergenziale, stiamo tornando al regime ordinario, anche se abbiamo in parte modificato la normativa dell'Ente per rendere più flessibile l'utilizzo di tale modalità di lavoro.

Mentre durante l'emergenza avevamo le persone attive in smart working per 4 o 5 giorni alla settimana, e per molte settimane consecutive, ora si torna ad avere una prevalenza del lavoro

svolto presso l'ufficio con un massimo di due giornate di lavoro agile alla settimana, fruibili, all'occorrenza, anche in modo continuativo nel mese.

L'esperienza fatta ha richiesto di rivedere processi, ripensare infrastrutture, o eravate già pronti?

Nel nostro caso eravamo pronti già prima del Covid19 in quanto lo smart working è iniziato in Regione Liguria nel 2018; ci stavamo già lavorando ma il progetto ha subito una brusca accelerazione a seguito della tragedia del crollo del Ponte Morandi.

L'emergenza sanitaria ha dato poi un forte impulso alla diffusione di questa modalità di lavoro. Dal punto di vista dell'infrastruttura tecnologica, in precedenza tutte le nostre persone in smart working avevano a disposizione

un sistema di VDI e quindi la possibilità di accedere da remoto, con le proprie credenziali, da qualunque PC, al loro ambiente di lavoro come se fossero in ufficio: banche dati, procedure, ecc.. Prima del Covid però il numero dei lavoratori che aveva aderito al progetto era modesto, meno di 100 smart worker, mentre con l'emergenza, avendo l'esigenza di mettere in



sicurezza i lavoratori, garantendo nel contempo la continuità delle attività amministrative, in pochissimi giorni siamo arrivati a ad oltre 1.200 lavoratori agili, di cui 400 in VDI e gli altri con accessi VPN. Quindi, erano tutti in condizione di accedere da remoto all'ambiente di lavoro allo stesso modo che in ufficio.

Inutile dire che lo smart working emergenziale ha dato una fortissima spinta alla digitalizzazione delle attività e allo sviluppo delle relative competenze; va considerato che l'età media nella PA è tipicamente alta, e molti dipendenti, se non vi fossero stati costretti, non avrebbero mai fatto questa esperienza.

Quanto è stata importante l'esperienza fatta in termini di digitalizzazione dei processi?

Abbiamo digitalizzato processi che sino ad allora sembravano condannati alla carta; prima ancora sono partiti processi già informatizzati che non riuscivano a decollare. Abbiamo e stiamo digitalizzando attività che prima richiedevano la presenza fisica e non erano remotizzabili. Così la formazione: in passato avevano soltanto alcuni corsi registrati fruibili on line, tutto il resto della formazione si svolgeva in presenza fisica. Nell'emergenza abbiamo confermato tutta la programmazione dei corsi di formazione che si sono però svolti a distanza, in modalità webinar, facendo registrare una maggiore partecipazione rispetto alla formazione d'aula. Per non parlare di riunioni, Giunte regionali, trattative sindacali, tutte svolte in modalità videoconferenza sulla piattaforma utilizzata dall'Ente.

Quindi la sua percezione è che non si tornerà indietro rispetto a quanto acquisito negli ultimi mesi...

A confermarlo è il tasso di adesione allo smart working nella Regione; prima accedevano a tale modalità meno di 100 dipendenti, oggi, in questa fase di ritorno al lavoro agile in modalità ordinaria, siamo già a 650 domande. Un aspetto che non dobbiamo dimenticare è che la pandemia da Covid19 ed il conseguente lockdown hanno costretto tante persone, direttori e dirigenti inclusi, a fare l'esperienza dello smart working e questo ha contribuito ad abbattere schemi mentali e resistenze culturali prima assai diffusi a tutti i livelli, non soltanto tra i dirigenti.

In molti hanno capito che lo smart working funziona, che si riesce a lavorare più concentrati e che per molte attività si è più efficienti. Ci sono Direttori, prima diffidenti, che oggi dichiarano che durante il lockdown tutte le attività sono state garantite nel rispetto delle scadenze e dirigenti che hanno ammesso che i propri collaboratori sono risultati più produttivi in modalità agile. In ogni modo smart working e lavoro in ufficio, meglio se smart office, sono complementari e servono entrambi.



Lo smart working è iniziato in Regione Liguria nel 2018; ci stavamo già lavorando ma il progetto ha subito una brusca accelerazione a seguito della tragedia del crollo del Ponte Morandi. L'emergenza sanitaria ha dato poi un forte impulso alla diffusione di questa modalità di lavoro. Prima del Covid però il numero dei lavoratori che aveva aderito al progetto era modesto, meno di 100 smart worker, mentre con l'emergenza siamo arrivati a ad oltre 1.200 lavoratori agili



IL CAFFÈ DIGITALE

ISCRIVITI ALLA NEWSLETTER MENSILE!

RICEVI GLI ARTICOLI
DEGLI ANALISTI DI THE
INNOVATION GROUP
E RESTA AGGIORNATO
SUI TEMI DEL MERCATO
DIGITALE IN ITALIA!

QUESTO MESE ABBIAMO
FATTO COLAZIONE CON...



COMPILA IL FORM DI REGISTRAZIONE SU
www.theinnovationgroup.it