MAGGIO 2020

IL CAFFÈ DIGITALE

THE INNOVATION GROUP NEWSLETTER

IL MERCATO DIGITALE NEL GOLFO DELL'INCERTEZZA

QUESTO MESE ABBIAMO FATTO COLAZIONE CON...

Michele RIVIERI
Chief Information Security Officer, Cedacri

IN PRIMO PIANO

IMMUNI facciamola presto... ma non basta!

LA TRASFORMAZIONE DIGITALE

Priorità delle PMI per la Ripartenza

CONNECTED MOBILITY

Il Contact Tracing per la ripresa della Mobilità

Sommario

L'EDITORIALE

Il mercato digitale nel golfo dell'incertezza 2
Roberto Masiero

IN PRIMO PIANO

IMMUNI facciamola presto…ma non basta! 7
Ezio Viola

NUMERI E MERCATI

Perché l'ICT sarà uno dei settori meno colpiti dalla crisi Covid-19 9
Carmen Camarca

LA TRASFORMAZIONE DIGITALE

Priorità delle PMI per la Ripartenza 11
Vincenzo D'Appollonio

Alle aziende conviene investire nella Trasformazione Digitale, migliora il Customer Engagement 13
Carmen Camarca

BANCHE E FINTECH

Fintech in Italia, un mercato già incerto prima dell'emergenza 15
Carmen Camarca

CYBERSEC E DINTORNI

Zoom e Smart Working: cosa abbiamo imparato 17
Elena Vaciago

CONNECTED MOBILITY

Il Contact Tracing per la ripresa della Mobilità 19
Elena Vaciago

DIRITTO ICT IN PILLOLE

Data tracing: le Linee Guida dell'EDPB costituiranno le basi dei trattamenti futuri 22
Valentina Frediani

VOCI DAL MERCATO

Il crisis management nei giorni del covid-19 24
Elena Vaciago

QUESTO MESE ABBIAMO FATTO COLAZIONE CON...

Michele RIVIERI
Chief Information Security Officer
Cedacri

CEDACRI GROUP

L'EDITORIALE

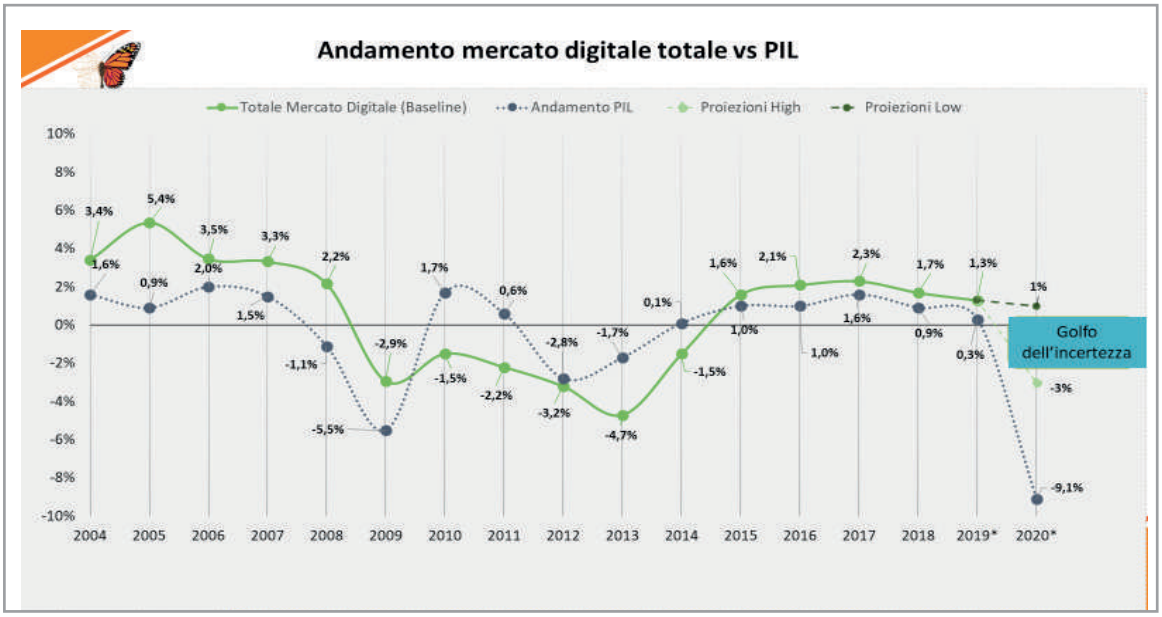
IL MERCATO DIGITALE NEL GOLFO DELL'INCERTEZZA

Roberto Masiero | Presidente, The Innovation Group

Il Coronavirus sta avendo un impatto drammatico non solo a livello sanitario, umano e sociale, ma sta anche determinando la più grave crisi economica globale dell'ultimo secolo. Alcuni autorevoli analisti prevedono che il Pil Italiano per il 2020 potrebbe subire una riduzione fino al 9%, e Confcommercio ipotizza uno scenario in cui 50.000 piccole imprese potrebbero essere costrette a chiudere, con una perdita di 300.000 posti di lavoro.

Eppure, queste tetre considerazioni non sembrano riflettersi automaticamente sulle prospettive del mercato digitale. Anzi, sembra di assistere al capovolgimento del paradosso di Solow, che negli anni 80' affermava "Si vedono computer ovunque tranne che nelle statistiche della produttività".

La Figura seguente mostra l'evoluzione delle dinamiche del PIL e del mercato digitale nel nostro Paese negli ultimi 15 anni (2004-2019).



Identifichiamo due momenti di maggiore discontinuità: la grande crisi del 2008, in conseguenza della quale il PIL subì una flessione del 5,5%, a fronte di una contrazione pari al 2,9 del mercato digitale; e

l'inversione del 2015, il primo anno in cui il mercato digitale tornò a registrare tassi di crescita superiori a quelli del PIL.

Pare dunque che il mercato digitale tenda ad avere un andamento sostanzialmente pro-ciclico rispetto al PIL.

risposte che si attendevano una riduzione del budget IT complessivo rispetto a quello precedentemente concordato, il 34% si aspettava invece un aumento parziale o addirittura "considerevole" del budget stesso (vedi Figura seguente).

La spiegazione potrebbe essere che, in anni in cui consumi e investimenti si contraevano, le aziende tendessero a tagliare gli investimenti in innovazione, che invece venivano rilanciati soprattutto dalle imprese più lungimiranti negli anni più floridi. Il che potrebbe farci prevedere, nel caso si avverasse la previsione di una flessione del PIL intorno al 9%, una contrazione simile in proporzione a quella avvenuta nel 2009, stimabile quindi intorno al 6%.

Ma alcuni indicatori fanno ritenere che per la prima volta potremmo assistere a una decisa inversione di tendenza, e a una sostanziale tenuta del mercato digitale, nonostante l'atteso crollo del PIL.

Una nostra ricerca sul campo, effettuata nelle scorse settimane intervistando CIO e CXO di 99 imprese italiane, ha fatto emergere risultati sorprendenti: in piena crisi del Coronavirus, con il Paese in stato di lock-down, a fronte del 29% di

> "Pochissime tra le grandi imprese hanno interrotto le attività. Le più avanzate erano già attrezzate per lo smart working e sono passate con relativa rapidità alla nuova modalità operativa"

Riteniamo non si tratti di un semplice "wishful thinking", ma di un vero e proprio cambiamento di natura del ruolo degli investimenti in digitale, che di fronte alla gravità della crisi vengono ad assumere una natura anticiclica.

A sostegno di ciò stanno alcune considerazioni che abbiamo rilevato nel corso di conversazioni con vari opinion leader ed executives del settore:

- Pochissime tra le grandi imprese hanno interrotto le attività.
  Le più avanzate erano già attrezzate per lo smart working e sono passate con relativa rapidità alla nuova modalità operativa.
  Alcune hanno addirittura raddoppiato i budget in IT per uscire dalla crisi con un maggiore vantaggio competitivo.
- L'esigenza di passare allo smart working e di sviluppare rapidamente soluzioni "quick & dirty" di e-commerce ha imposto a molte medie

aziende scelte e investimenti che venivano posticipate da anni

- Il dramma del Coronavirus, le migliaia di perdite di vite umane che eroici medici ed infermieri hanno tentato di contrastare a mani nude, il fiorire di creatività nella didattica guidato da migliaia di insegnanti che tentano di supplire dal basso all'inadeguatezza degli strumenti a loro disposizione impongono un salto di qualità negli investimenti della Pubblica Amministrazione in aree chiave come la scuola e la Sanità.

Sulla base delle informazioni raccolte, riteniamo ragionevole la stima per cui, proprio per la natura anticiclica che essa viene oggi ad assumere, la spesa in digitale nel corso del 2020 potrebbe addirittura registrare un moderato incremento, nell'ordine dell'1%.

Tre fattori potrebbero intervenire tuttavia a peggiorare questo risultato:

- Il 40% della spesa in IT è generato da Piccole e Medie Imprese, e in particolare moltissime microimprese rischiano di rappresentare il ventre molle del sistema e di venire travolte dalla crisi, senza avere la capacità, ma nemmeno la possibilità, di quello scatto di reni che potrebbe consentire loro di inserirsi in un mercato in rapidissima trasformazione;
- La rapida implementazione del 5G, al di fuori della fase di sperimentazione, è condizione essenziale per il deployment di applicazioni essenziali per il miglioramento della produttività delle imprese e dell'efficacia dei servizi pubblici.
- La dilazione nel lancio dei nuovi progetti da parte della PA, la cui fisiologica lentezza è aggravata dal funzionamento molto parziale dello smart working in regime di lockdown.

Anche in considerazione di questi possibili fattori inibitori riteniamo di poter prevedere il "worst case" in una forchetta tra una crescita dell'1% – in cui confidiamo – e una flessione del 3%: è quello che noi definiamo "il golfo dell'incertezza" che abbiamo di fronte.

In un recente convegno, Marco Bentivogli affermava amaramente: "Il problema del paese è di essere prigioniero di tecnofobi ignoranti". Alle élites intellettuali e professionali di questo Paese il compito di trasformare questa crisi in un'occasione di crescita sociale ed economica per tutti noi.

QUESTO MESE ABBIAMO FATTO COLAZIONE CON

La sicurezza declinata su banche di ogni dimensione

Intervista di **Roberto Bonino** a
Michele Rivieri
Chief Information Security Officer di Cedacri

Non è una banca in senso stretto, ma deve pensare e spesso agire come una banca. Anzi, come tante banche e istituzioni finanziarie che a essa si affidano per la gestione dei sistemi informativi.

Stiamo parlando di Cedacri, realtà italiana di riferimento nei servizi di outsourcing informatico per il settore bancario, con un fatturato superiore ai 270 milioni di euro e oltre 800 dipendenti perlopiù impegnati a supportare un parco di oltre 100 clienti, che comprende anche diverse istituzioni finanziarie, aziende industriali e società di servizi.

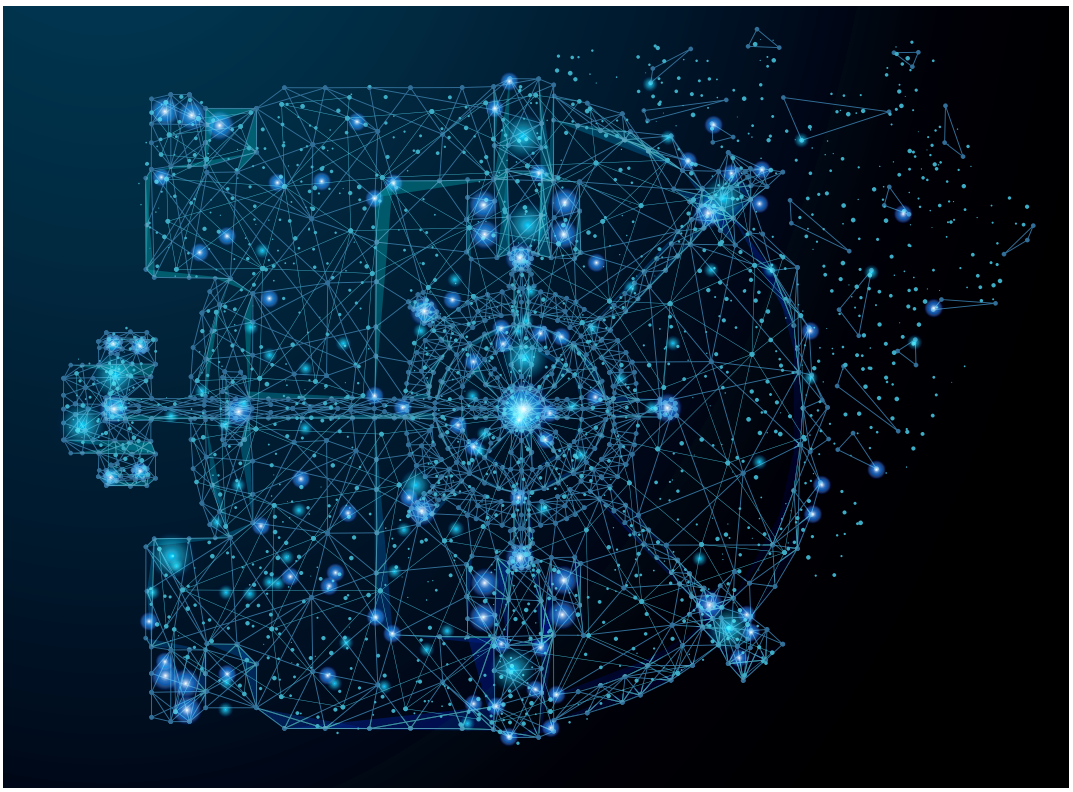
Nel proprio ruolo di outsourcer, Cedacri spesso gestisce in modo integrale i sistemi informativi soprattutto di banche territoriali, che non dispongono di competenze e risorse sufficienti per occuparsi della componente tecnologica.

La sicurezza è uno degli aspetti più delicati per un comparto oggetto di continui attacchi e molto appetibile per il cybercrime organizzato: "Gli istituti di dimensioni più ridotte si trovano a vivere il paradosso di dover ottemperare a normative pensate per proteggere le realtà più complesse", spiega Michele Rivieri, Chief Information Security Officer di Cedacri. "Oggettivamente, parliamo di soggetti esposti a pericoli reali in misura spesso minore rispetto ai nomi di riferimento del panorama finanziario italiano, ma gli obblighi di compliance sono uguali per tutti, con oneri economici complessi da gestire per chi non può far leva su budget troppo significativi".

Questo scenario conferma come il tema della sicurezza non debba essere trascurato dalle banche di piccole e medie dimensioni. O almeno non dovrebbe.

La realtà, fotografata in una recente indagine qualitativa condotta da Indigo Communication, evidenzia tratti a volte contraddittori, soprattutto in termini di consapevolezza delle problematiche da affrontare. In linea generale, gli investimenti messi in campo negli anni hanno consentito in buona misura di raggiungere uno standard considerato elevato sul fronte della protezione perimetrale, mentre piuttosto diffusa è la preoccupazione riferita soprattutto ai servizi di Internet banking e al comportamento del personale interno, in quest'ultimo caso per prevenire tentativi di frode che facciano leva su phishing e social engineering.

Tuttavia, nell'universo di riferimento di Cedacri verosimilmente rappresentativo di tutta la realtà italiana, solo una percentuale minoritaria di



istituti dispone di figure interne specializzate nella sicurezza informatica e, quindi, più attente alle evoluzioni in materia: "Non è una situazione così sorprendente", rileva Rivieri. "In molti casi abbiamo un ruolo da full outsourcer ed è quindi normale che istituti di piccole e medie dimensioni, concentrate sulla loro operatività, deleghino a noi impostazioni strategiche, scelte e aggiornamenti in ambito sicurezza informatica".

Cedacri funge anche da vero e proprio Soc (Security Operation Center) per le banche totalmente appoggiate ai propri servizi e, in generale, per un'ampia maggioranza delle oltre 60 realtà gestite, imposta il piano di sicurezza ed effettua tutte le scelte tecnologiche correlate: "I soggetti di dimensione media, per i quali svolgiamo solo una parte delle attività, dispongono di una struttura It più articolata, spesso con un gruppo di sviluppatori interno, e quindi godono anche di maggior autonomia", specifica Rivieri.

Nell'attuale scenario della sicurezza informatica, appare inevitabile avere un approccio reattivo di fronte alle minacce in continua evoluzione: "Nel nostro gruppo operano specialisti incaricati di fare monitoraggio continuo, rilevazione delle anomalie, analisi e comprensione delle motivazioni", illustra Rivieri. "Per competere con gli attaccanti, occorre fare bene le sentinelle e non illudersi di essere protetti solo perché si ritiene di avere il perimetro ben protetto. Spesso il punto debole è rappresentato dal comportamento umano ed è lì che vanno a insistere i malintenzionati.

Avere buone pratiche di sicurezza, oggi, significa soprattutto saper rilevare rapidamente un tentativo di intrusione e porvi gli adeguati rimedi". Il fattore umano rappresenta l'elemento più critico nella misurazione dell'efficacia di una strategia di sicurezza e questo riguarda le aziende di ogni dimensione. Gli investimenti in formazione non andrebbero lesinati, ma inevitabilmente, più ci si confronta con realtà poco strutturate, più si avverte la fatica di garantire il livello di preparazione che servirebbe. Poiché la responsabilità delle scelte su questo fronte resta di pertinenza delle singole banche, Cedacri nel suo piano strategico ha previsto di rafforzare le attività di Soc: "Vogliamo aiutare i nostri clienti a migliorare il livello complessivo della loro sicurezza e, a tal fine, rappresenta un forte vantaggio avere, come SOC, una visione a tutto tondo della infrastruttura informatica della banca, sia la parte gestita direttamente da Cedacri che quella mantenuta presso le sedi del cliente", conclude Rivieri.

CEDACRI FUNGE ANCHE DA VERO E PROPRIO SOC (SECURITY OPERATION CENTER) PER LE BANCHE TOTALMENTE APPOGGIATE AI PROPRI SERVIZI

IN PRIMO PIANO

IMMUNI
facciamola presto…ma non basta!

Ezio Viola
Managing Director, The Innovation Group

Dopo il lavoro svolto dalla task force per valutare le tecnologie da usare per combattere l'epidemia da coronavirus, il Ministero dell'Innovazione ha pubblicato pochi giorni fa i documenti a supporto della scelta della app di contact tracing da utilizzare nella fase 2 dell'emergenza Covid-19.

Per settimane questi documenti sono rimasti secretati e solo adesso sono stati quindi pubblicati. Il documento risale a quasi un mese fa e se fosse stato reso noto prima, avrebbe evitato analisi e valutazioni sui media inutili e a volte premature e sbagliate. Gli esperti della task force, tenendo conto anche dei tempi messi a loro disposizione, hanno fatto un lavoro dal punto di vista tecnico serio e ben argomentato, evidenziando limiti, vincoli, interventi necessari e raccomandazioni da seguire nella fase implementativa successiva alla scelta. Ci sono alcune sorprese leggendo i documenti se paragonate con le scelte fatte successivamente dal Governo. Il lavoro presentato non arriva infatti a determinare i criteri che poi hanno portato alla scelta di Immuni da parte del Governo come app ufficiale per il tracciamento dei contagi. Le raccomandazioni della task force indicano infatti ad esempio di testare in via parallela due app, Immuni e CovidApp, un'altra soluzione proposta. Il Governo ha deciso di non seguire questa raccomandazione e di fare una scelta senza una fase di test per entrambe. La task force aveva indicato che la scelta della app fosse preceduta da un test per verificare una serie di requisiti tecnici che al momento della realizzazione del report non erano rispettati appieno da nessuna delle due app indicate. Dalla preparazione del report per il Governo molte cose sono cambiate e Immuni ora dovrebbe essere una soluzione più completa, compreso l'allineamento dell'app ai requisiti tecnici realizzati da Apple e Google sulle

> Dalla preparazione del report per il Governo molte cose sono cambiate e Immuni ora dovrebbe essere una soluzione più completa, compreso l'allineamento dell'app ai requisiti tecnici realizzati da Apple e Google sulle piattaforme di sistema operativo degli smartphone utilizzati dal 90% della popolazione.

loro piattaforme di sistema operativo degli smartphone utilizzati dal 90% della popolazione.

Inoltre, è notizia recente che le due società pubbliche che gestiranno rispettivamente i dati e la tecnologia di Immuni saranno Sogei e PagoPA.

Inoltre, ciò che è scritto nel documento degli esperti è la parte più importante e di cui poco si parla per evitare, come è già accaduto in passato quando si progettano sistemi e app, di badare al front-end e dimenticare i processi a monte e a valle perché funzioni operativamente.

Riprendo quindi una sintesi delle raccomandazioni finali così come sono nel documento:

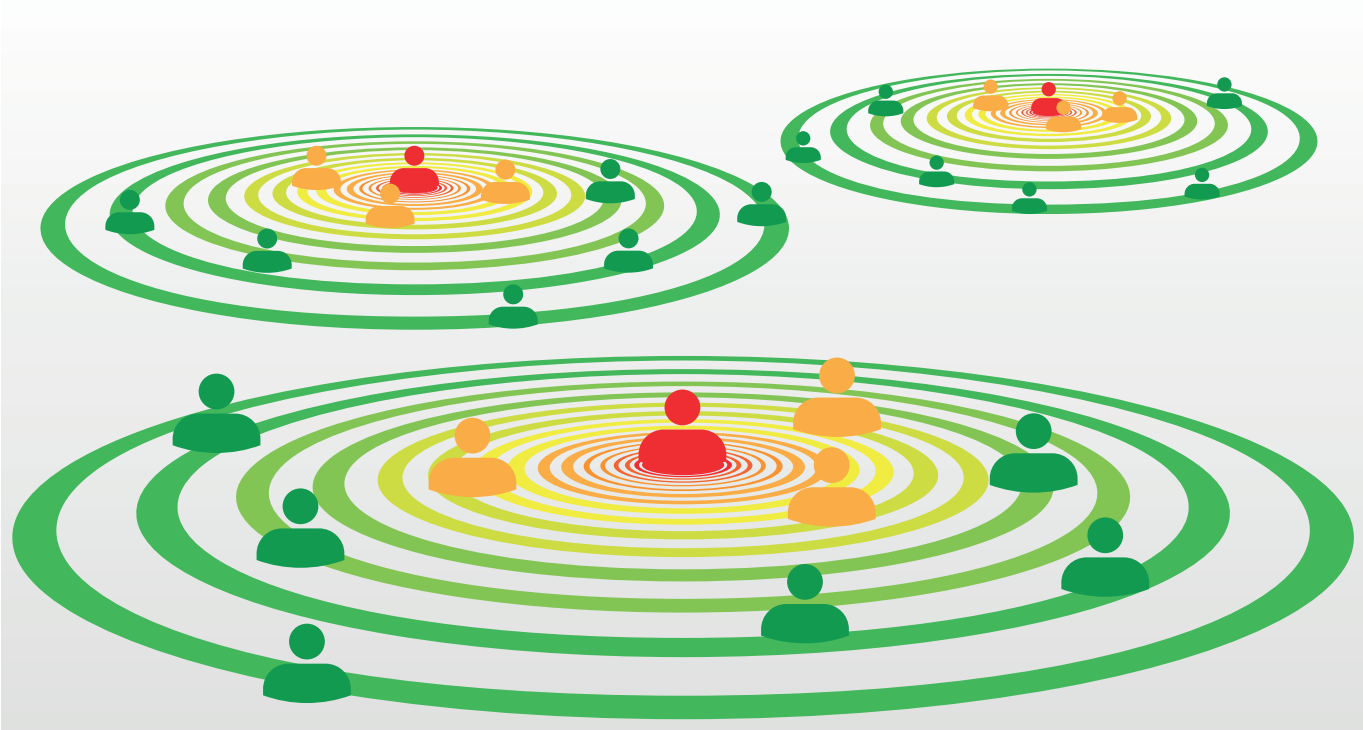
"La proposizione della soluzione tecnologica per il contact-tracing che uscirà vincente ai test, prima di essere implementata sul campo, dovrebbe infine essere calata in un quadro strategico-organizzativo più ampio a carico del decisore politico, il quale, per controllare la trasmissione dei contagi, dovrebbe tenere in considerazione non solo altre misure di prevenzione, in aggiunta a quelle basate su soluzioni tecnologiche per il contact tracing ma anche strategie di azione di carattere generale".

Inoltre, vengono esplicitate e richieste alle autorità pubbliche alcune decisioni importanti per mettere in esercizio il sistema di contact tracing.

Nominare un Program Manager e scegliere tra le principali opzioni tecnico-organizzative che impattano su questioni chiave di salute pubblica e di tutela della privacy.

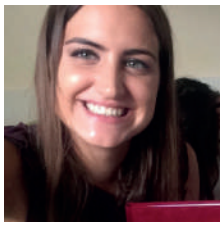
- Policy per le tecnologie di contact tracing. I sistemi di tracing e le proposte selezionate possono avvalersi di strumenti di rilevazione dei contatti che hanno diversi livelli di impatto atteso sull'efficacia degli interventi di salute pubblica e sul trattamento dei dati personali.
- Policy da applicare per allertamento a seguito di contagio. Nel caso in cui un cittadino dotato di app risultasse positivo ai test, è possibile attivare due diverse procedure di allertamento attraverso una procedura volontaria e manuale o una pre-autorizzata e automatica.
- Policy da applicare per garantire l'enforcement delle azioni di carattere sanitario conseguenti. A seguito della rilevazione di un caso positivo e dell'allertamento dei soggetti con cui è entrato in contatto, devono seguire azioni di carattere sanitario (ad esempio la quarantena e/o l'autoisolamento per i soggetti entrati in contatto con il caso positivo), che possano essere intraprese anch'esse con procedura volontaria e proattiva.

Queste scelte sono fondamentali e gli impatti in termini di risorse e tempi necessari per realizzarle sono critiche. Rimaniamo quindi in attesa del piano operativo e speriamo che adesso il Governo e il Ministero cessino di secretare i documenti dei loro stessi esperti e imbocchino la strada della completa trasparenza. Se vogliamo avere la speranza che l' app sia adottata da gran parte della popolazione e che abbia una qualche efficacia, i cittadini devono potersi fidare e senza fiducia Immuni sarà un fiasco.



NUMERI E MERCATI

Perché l'ICT sarà uno dei settori meno colpiti dalla crisi Covid-19



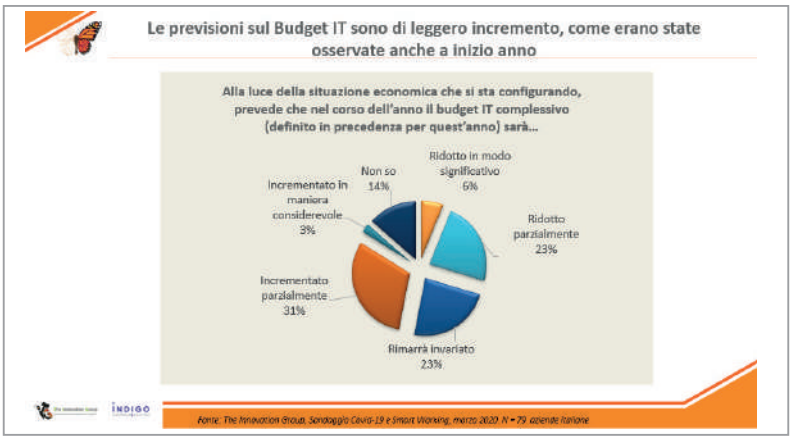
Carmen Camarca
Analyst, The Innovation Group

Nonostante la situazione difficile che stanno affrontando, le aziende prevedono per quest'anno un aumento (anche se parziale) del budget IT.

Lo riporta un recente sondaggio[1] condotto da The Innovation Group volto, appunto, a comprendere l'impatto del coronavirus sul business aziendale e la diffusione dello Smart Working in seguito alla situazione di emergenza.

Dall'analisi, infatti, emerge che per il 31% dei rispondenti nel 2020 la propria azienda aumenterà, seppur di poco, il budget IT contro il 23% secondo cui rimarrà invariato e il 29% che ne prevede una riduzione (per il 6% dei quali significativa).

È, infine, il 3% del campione a ritenere che il budget IT della propria azienda aumenterà in maniera significativa. I risultati non differiscono da quanto emerso dalla Digital Business Transformation Survey[2], analisi annuale di The Innovation Group che studia la diffusione della trasformazione digitale nelle aziende italiane e condotta prima del verificarsi della situazione di emergenza.



Secondo la rilevazione il 40% del campione, già prima dello scoppio della pandemia, dichiarava che il budget IT della propria azienda sarebbe aumentato nel corso dell'anno, mentre per la metà dei rispondenti sarebbe rimasto invariato e per il 10% diminuito.

Ma perché nonostante la situazione

critica e il lockdown (che ha imposto la chiusura di molte attività produttive) le previsioni di spesa IT non cambiano? Se la riduzione delle revenue impone una rivisitazione dei propri piani di investimento perché le aziende decidono di investire comunque in IT?

La risposta è, in parte, nella diffusione dello Smart Working ma, soprattutto, nel valore aggiunto che per molte aziende ha rappresentato l'adozione delle soluzioni tecnologiche nell'affrontare la crisi, inducendo ad una riconsiderazione degli attuali modelli di business.

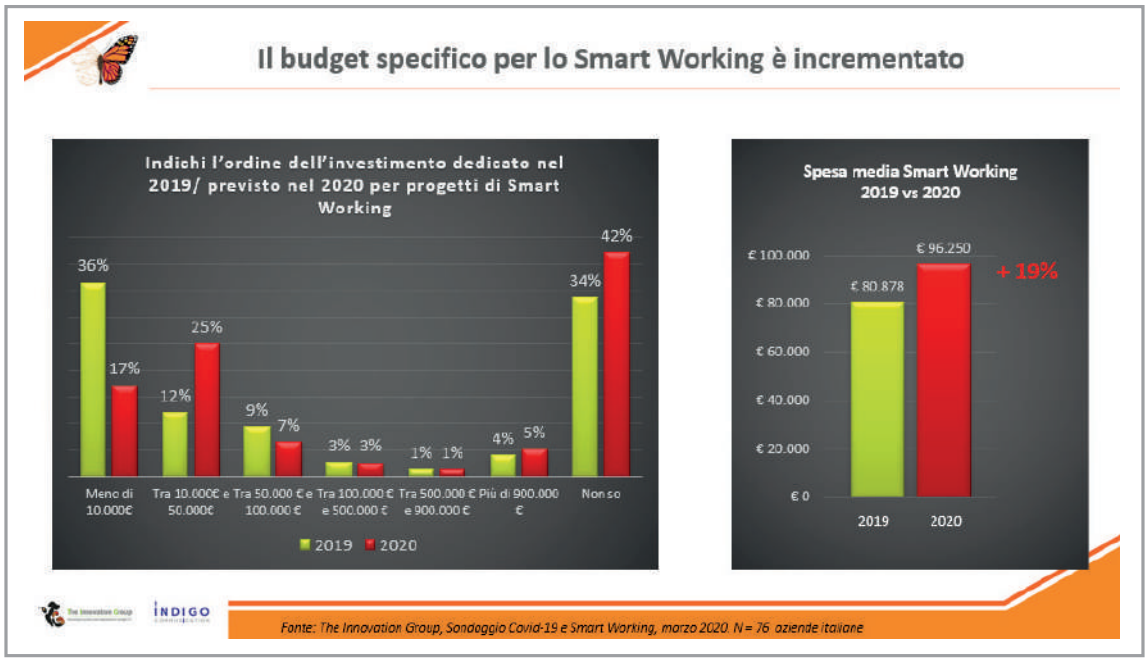
L'analisi ha mostrato, infatti, come dal 2019 al 2020 la spesa in Smart Working sia aumentata del 19%, passando da un investimento medio del 2019 di quasi 81mila euro ad uno di poco più di 96mila nel 2020.

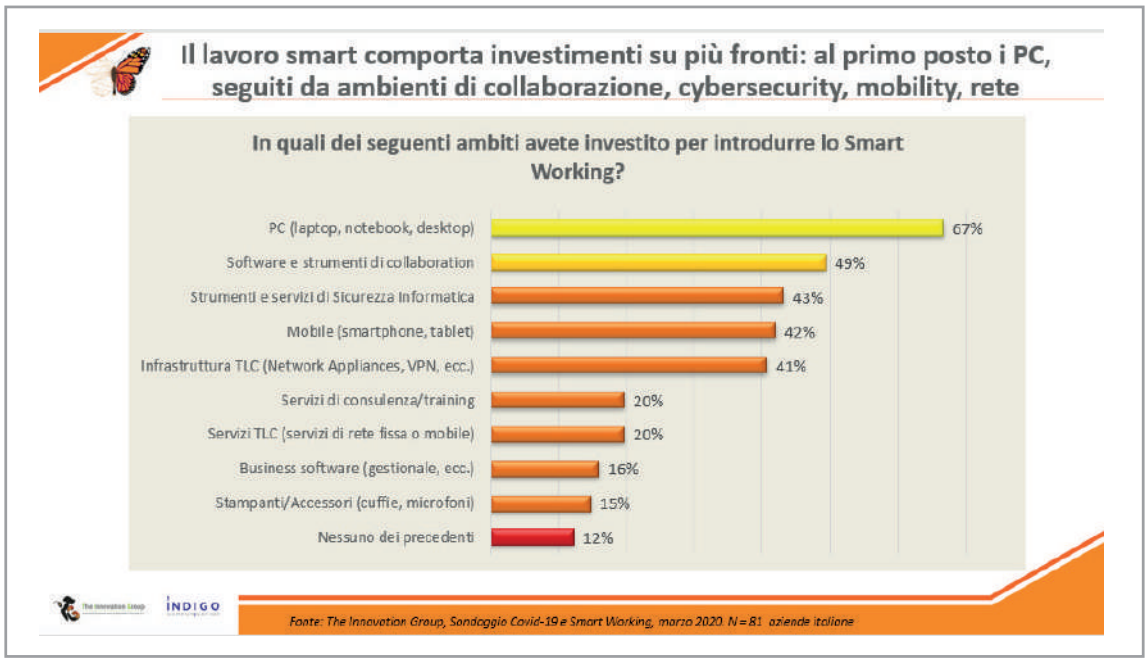
Dal 2019 al 2020 è, inoltre, diminuita del 53% la percentuale di chi dichiara di dedicare allo Smart Working un budget di meno di 10.000 euro a favore di chi prevede una spesa compresa tra 10.000 e 50.000 euro (+108% su base annua).

Nel dettaglio, per introdurre lo Smart Working al proprio interno, le aziende hanno investito principalmente in Pc, laptop, notebook e desktop (67% dei rispondenti) e in software e strumenti di collaborazione (49%).

Oltre il 40% del campione ha, inoltre, dichiarato di aver investito in strumenti e servizi di sicurezza informatica, in ambito mobile e in infrastruttura TLC.

La propensione ad aumentare gli investimenti in ICT è un trend rilevato anche da un'indagine realizzata dall'istituto di ricerche Astraricerche in collaborazione con Manageritalia e Cfmt – Centro di Formazione Management del Terziario secondo cui, appunto, dopo la crisi gli investimenti aziendali saranno uguali o addirittura in aumento che in precedenza e il settore ICT sarà quello meno impattato dalla situazione critica che stiamo affrontando (per il 52% del campione sarà uno degli ambiti di maggiore investimento).





[1] Il sondaggio, dal titolo "Impatto dell'emergenza Coronavirus e Smart Working", è stato condotto da The Innovation Group tra marzo e aprile 2020 su 99 aziende italiane.

[2] La Digital Business Transformation Survey è stata condotta da The Innovation Group tra dicembre 2019 e febbraio 2020 su un campione di 181 aziende italiane.

LA TRASFORMAZIONE DIGITALE

Priorità delle PMI per la Ripartenza

Vincenzo D'Appollonio
Partner, The Innovation Group

Anche in questo periodo di emergenza sociale determinata dalla epidemia Covid-19, ho modo di continuare in 'smart-working' le mie attività di Consulenza Direzionale come Innovation Manager con le PMI lombarde, ed ho raccolto le loro priorità, in termini di azioni e bisogni, per sostenere una ripartenza il più possibile pronta, efficiente ed efficace: vediamo le più importanti.

Messa in sicurezza

Governo e parti sociali (Cgil, Cisl, Uil, Confindustria e Confapi) si sono accordati per garantire la sicurezza dei luoghi di lavoro delle aziende, seguendo la 'tabella dell'Inail' che classifica i livelli di rischio per i dipendenti.

E dunque saranno pronte per la ripartenza le imprese che avranno dimostrato di poter rispettare protocolli di sicurezza quali distanziamento di almeno un metro, dotazione di dispositivi di protezione come guanti e mascherine, pulizia due volte al giorno, dispenser di disinfettanti agli ingressi e vicino ai computer, sanificazione dei sistemi di areazione, 'smart-working' per il maggior numero di dipendenti, orari differenziati per gli altri: tutto ciò sta richiedendo alle imprese uno sforzo organizzativo e una capacità di investimento assolutamente straordinari.

Filiera dei pagamenti virtuosa

Nella situazione di emergenza drammatica che stiamo vivendo, l'unica possibile via di uscita è una strategia basata sulla coesione sociale.

E ciò vale soprattutto per il sistema delle imprese, dove c'è il rischio che con il 'corto circuito' dei pagamenti scompaiano interi pezzi delle filiere produttive, generando un danno in prospettiva ancora più grave.

Un atteggiamento ingiustificato di mancato rispetto delle scadenze può produrre una crisi di liquidità ed un conseguente effetto 'domino' in grado di fare uscire dal mercato entità produttive già deboli finanziariamente, ma indispensabili all'ordinato funzionamento del sistema-filiera nel suo complesso: dunque chi può onorare i debiti deve farlo, adesso è necessario far prevalere la responsabilità e la solidarietà nei confronti di tutti i creditori, dalle aziende ai professionisti.

Liquidità, sostegno finanziario alla ripresa

Quella conseguente alla diffusione del COVID-19 è anche una forte crisi economica che sta interessando direttamente l'economia reale e che potrebbe estendersi al settore bancario e finanziario a causa delle difficoltà in cui le imprese potrebbero incorrere nel far fronte ai propri obblighi di pagamento, ed alle proprie necessità di finanziare la ripartenza.

Governo, Regioni ed Associazioni di categoria come l'ABI hanno già definito alcuni interventi e misure finalizzate a dare sostegno alle imprese, quali il potenziamento del Fondo di

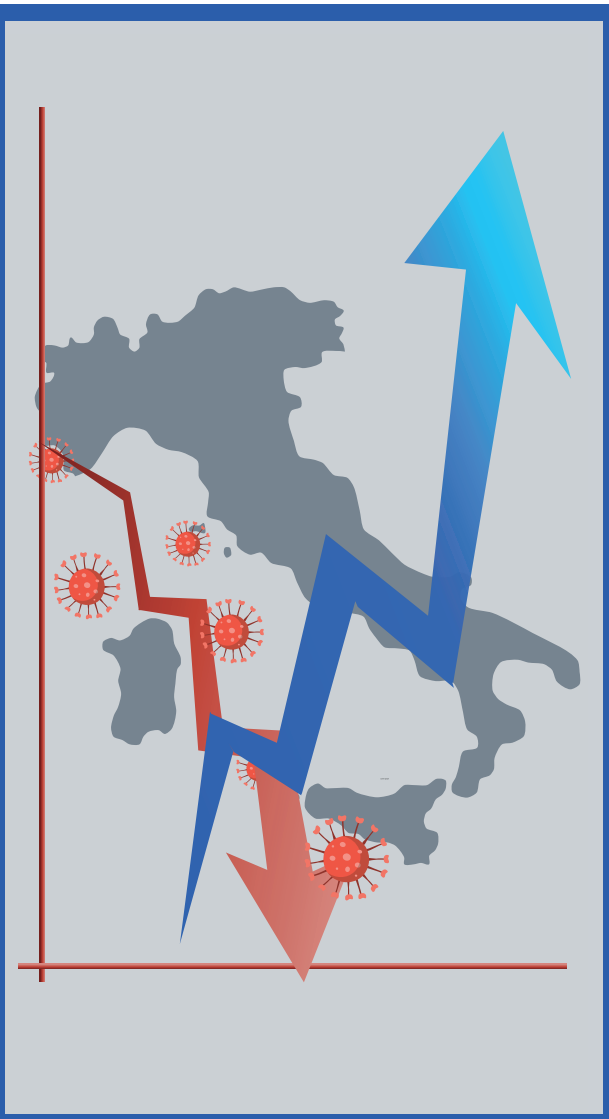
Garanzia per le PMI, con la moratoria statale per i finanziamenti ed il sostegno alla nuova finanza; i Fondi Regionali per la Ripresa, che un numero crescente di regioni sta mettendo in campo con una serie di misure per sostenere imprese e famiglie alle prese con i danni causati dall'emergenza Covid-19; l'Addendum all'Accordo per il Credito 2019, con la moratoria ABI e l'estensione del programma 'Imprese in Ripresa 2.0': occorre ora soprattutto rapidità d'intervento per erogare al più presto 'liquidità' alle imprese, ed evitare così che l'emergenza economico/finanziaria della cosiddetta 'Covidnomics' venga aggravata da una emergenza 'burocratica'.

Trasformazione del modello di business

L'emergenza Covid-19 che stiamo vivendo impone alle aziende una profonda revisione del proprio modello di business, ed implica una trasformazione organizzativa, tecnologica e digitale. La trasformazione del proprio business deve avvenire oggi accogliendo ed applicando in azienda l'innovazione nel modo più aggressivo, nella prospettiva di una Ripartenza che deve essere vista come opportunità di sviluppo di nuovi modelli organizzativi e collaborativi, di nuovi prodotti e servizi, e di crescita sul Mercato.

Occorre subito sviluppare un Business Plan COVID triennale, con l'obiettivo di definire un percorso di evoluzione del modello di business dopo la fase di emergenza, presidiando il proprio 'modus operandi' tradizionale ma continuando ad innovare e spostando in modo progressivo il proprio posizionamento strategico, beneficiando di quelle azioni di riduzione dei costi fissi, agevolazioni finanziarie e valorizzazione di opportunità che l'emergenza mette a disposizione, sia in termini di mercato che di supply-chain.

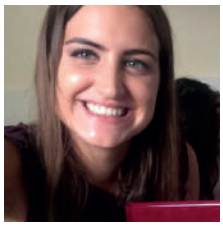
The Innovation Group è stata iscritta nell'ottobre 2019 dal Ministero dello Sviluppo Economico nell'apposito Albo delle Società di Consulenza qualificate come fornitrici esclusive, sul territorio nazionale, di servizi consulenziali di 'Innovation Management'. The Innovation Group è dunque oggi pronta a fornire alle imprese "servizi di consulenza specialistica finalizzati a sostenere processi di innovazione negli ambiti della trasformazione tecnologica e digitale, ammodernamento degli assetti gestionali e organizzativi, accesso ai mercati finanziari e dei capitali", per assistere operativamente le PMI nello sviluppo dei loro Business Plan per la Ripartenza e sostenerle nel percorso di raggiungimento dei loro nuovi obiettivi strategici: lavorando insieme vinceremo anche questa nuova sfida!



Occorre subito sviluppare un Business Plan COVID triennale, con l'obiettivo di definire un percorso di evoluzione del modello di business dopo la fase di emergenza, presidiando il proprio 'modus operandi' tradizionale ma continuando ad innovare e spostando in modo progressivo il proprio posizionamento strategico

LA TRASFORMAZIONE DIGITALE

Alle aziende conviene investire nella Trasformazione Digitale, migliora il Customer Engagement



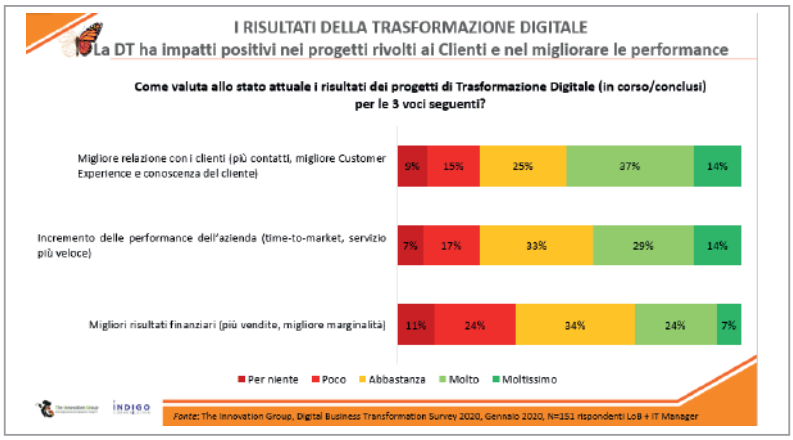
Carmen Camarca
Analyst, The Innovation Group

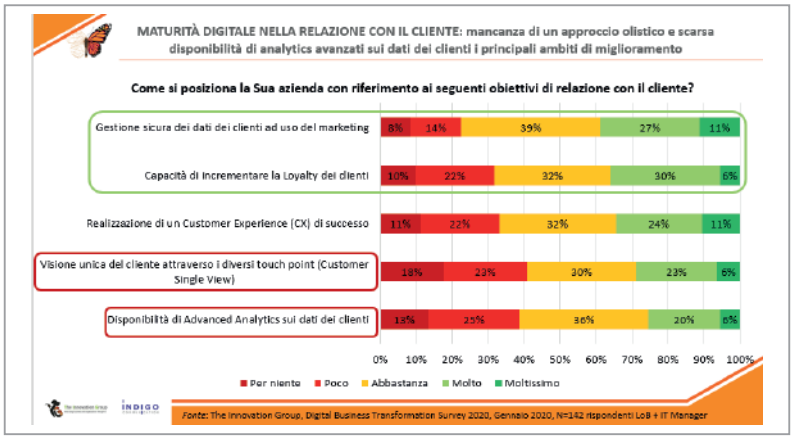
Promuovere la trasformazione digitale in azienda vuol dire innanzitutto migliorare la relazione con il cliente, conoscerlo meglio, riuscire ad intercettare le sue preferenze con facilità e aumentarne, quindi, la Customer Experience.

È quanto è emerso dalla Digital Business Transformation Survey condotta da The Innovation Group tra dicembre 2019 e gennaio 2020 su un campione di 184 LoB e IT manager.

In particolare, la metà del campione (51%) valuta molto positivamente l'impatto che le strategie di trasformazione digitale hanno avuto sulla relazione con i propri clienti, a fronte di un 24% che si esprime in maniera negativa.

Tra le altre attività prese in considerazione, secondo il 43% dei rispondenti la trasformazione digitale comporta, inoltre, un incremento dell'efficienza delle performance aziendali mentre il 31% ritiene che migliori le performance finanziarie.





Per quanto riguarda le attività sui clienti, per il 38% del campione la propria azienda ne gestisce in maniera sicura i dati mentre il 36% considera molto buone le capacità di incrementarne la loyalty e il livello di fidelizzazione.

A ritenerlo sono principalmente aziende di piccole dimensioni (meno

di 99 dipendenti) attive in ambito ICT/TLC e Servizi.

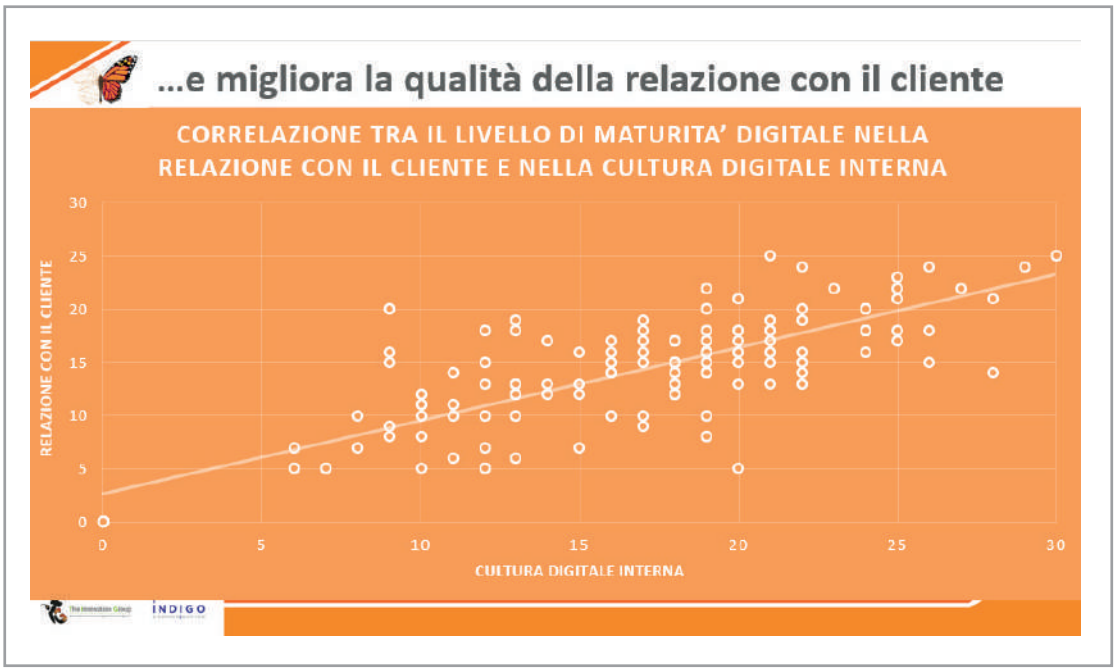
Tuttavia, per le aziende è ancora difficile riuscire ad adottare un approccio olistico che permetta una lettura integrata dei dati e delle informazioni dei propri clienti ricavabili dai diversi punti di contatto digitali.

La problematica, avvertita dal 41% del campione, si accompagna alla scarsa disponibilità di strumenti di Advanced Analytics (38%): in entrambi i casi si tratta perlopiù di aziende di piccole dimensioni appartenenti ai settori dell'Industria e della Pubblica Amministrazione.

Se, quindi, da un lato le aziende riescono a garantire un utilizzo sicuro dei dati dei propri clienti, individuando le migliori strategie per aumentarne l'engagement, dall'altro emerge ancora la forte necessità di adottare una customer single view e di saper leggere e interpretare correttamente le informazioni degli utenti.

Si tratta di una lacuna, emersa anche dalle precedenti edizioni della survey, su cui è necessario che le aziende intervengano in tempi rapidi, soprattutto se si considera che multicanalità e analytics sono ormai universalmente riconosciute come le principali strategie da adottare nei prossimi anni per avere successo con i clienti.

Dalla survey è, infine, emerso che anche la cultura aziendale incide positivamente sulla relazione con il cliente.



Infatti, un aumento del livello della cultura digitale interna (intesa come ubiquità delle informazioni, always on del dipendente, knowledge sharing, empowerment del dipendente, promozione di iniziative data driven) comporta un miglioramento della qualità della relazione con i clienti.

RIUSCIRE AD INSTAURARE CON IL CLIENTE UN RAPPORTO DI QUALITÀ È UN OBIETTIVO STRATEGICO CHE COINVOLGE L'AZIENDA IN DIVERSE AREE

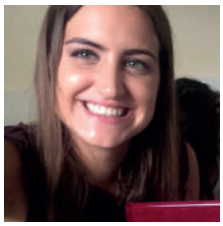
Che la trasformazione digitale permettesse di creare un nuovo tipo di relazione con i clienti era ormai noto ma che questa dipendesse anche dallo sviluppo in azienda di una determinata cultura è una novità.

Riuscire ad instaurare, quindi, con il cliente un rapporto di qualità è un obiettivo strategico che coinvolge l'azienda in diverse aree e che richiede un impegno del management a più livelli.

Il Customer Engagement del cliente richiede innanzitutto adottare una nuova visione in azienda e, soltanto in un secondo momento, mettere in campo le strategie e gli strumenti tecnologici per far sì che ciò avvenga nella maniera più efficace possibile.

BANCHE E FINTECH

Fintech in Italia, un mercato già incerto prima dell'emergenza



Carmen Camarca
Analyst, The Innovation Group

Sebbene in Italia la diffusione delle Fintech sia avvenuta cinque anni dopo l'affermazione del fenomeno nel mondo, l'interesse per queste realtà è andato aumentando di anno in anno, anche se poi è soltanto dal 2018 che il mercato italiano ha subito una forte accelerazione, soprattutto in seguito all'introduzione della PSD2, entrata in vigore a settembre 2019.

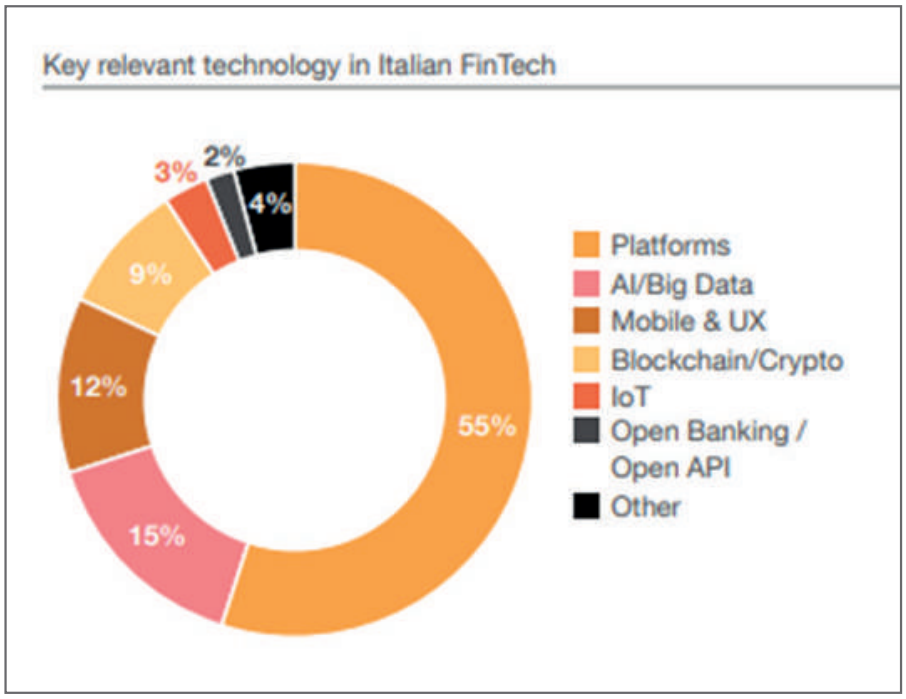
A dirlo è il report "Fintech 2020" pubblicato lo scorso aprile da Pwc[1] secondo cui in Italia si verificherà uno scenario maturo soltanto nei prossimi 3/5 anni (entro il 2025).

In particolare, le fintech censite sono 278, 49 in più rispetto all'edizione precedente del report, appartenenti a diversi settori di mercato (anche questi in aumento rispetto agli scorsi anni con l'ingresso dei segmenti Real Estate, Criptovalute e investimenti specializzati in NPL).

Ad ogni modo è il payment il segmento di maggior dinamismo, all'interno del quale il numero di fintech continua a crescere.

Per quanto riguarda la componente tecnologica, oltre al ruolo rilevante detenuto dalle piattaforme, emerge che sta crescendo anche l'utilizzo dell'Artificial Intelligence, intesa soprattutto come Advanced Analytics e Big Data, soluzioni di cui si dispone soprattutto nell'ambito del money management e del payment.

In crescita anche l'applicazione della Blockchain, soprattutto nel mercato del trading, negli investimenti dedicati alle criptovalute e nel Wealth management.



Soltanto in minima parte le Fintech si avvalgono dell'IoT, utilizzato soprattutto nell'Insurtech, mentre soltanto di recente si stanno sviluppando i primi esperimenti nel campo dei pagamenti.

Cresce, infine, anche il fatturato (che nel 2018 raggiunge 373 milioni di euro, con una crescita del 40% su base annua) e la quota delle scaleup (le società che hanno almeno un milione di euro di fatturato, che passano dalle 28 del 2019 alle 37 del 2020, registrando un + 32%).

Dallo studio emerge, tuttavia, che in Italia sono ancora troppo limitati gli investimenti nel settore, una problematica da cui deriva anche il debole posizionamento del nostro Paese nel panorama internazionale: nel 2019, infatti, gli investimenti si sono ridotti del 22%, la maggior parte dei quali a favore delle realtà più consolidate e di maggiori dimensioni.

Key numbers of Payments compared to FinTech total

	Payments	Total FinTech
number of companies	**46**	**278**
% on Total	17%	100%
growth 2019-2018	28%	21%
revenues (% on Total)	**35%**	**100%**
growth 2018/2017	62%	40%
average revenues	4.4€	2.1€
N° of scale up (% on each segment)	20%	13%
average age (years)	**4.4**	**4.8**
Investments (% on Total)	**10%**	**100%**
EBITDA	**-9%**	**2%**

▲ ▼ ~

L'impatto del coronavirus

Nel report si fa accenno anche agli impatti del coronavirus sul mercato.

Al proposito le principali preoccupazioni riguardano gli investimenti del Venture Capital che probabilmente potrebbero accentuare il divario tra le startup, comportando una minore attenzione verso le nuove startup.

Si prevede un effetto negativo anche per il volume delle transazioni, che potrebbe portare a una diminuzione dei profitti e degli investimenti nel comparto.

Va comunque sottolineato che durante il lockdown la possibilità di svolgere pagamenti da remoto e di acquistare online si è rivelata di estrema utilità, una dinamica positiva in realtà già evidenziata dal report che riportava appunto come, lo scorso anno, il settore dei pagamenti fosse cresciuto del 28%, rappresentando il 17% del mercato totale.

Secondo un recente studio condotto dagli analisti di SumUp, società di fintech basata a Londra, dallo scorso marzo ad oggi in Italia è triplicato il volume dei pagamenti digitali da parte dei piccoli commercianti, arrivando a registrare picchi di incremento del 350%.

L'emergenza, quindi, costringendo i piccoli commercianti a individuare soluzioni concrete per scongiurare un blocco dell'attività produttiva, ha ampliato l'ambito del digital payment ad un nuovo target di clientela, intercettando così un'utenza che, oltre ad essere quella finora più restia ad adottare le nuove soluzioni è anche quella di maggior rappresentanza del commercio italiano.

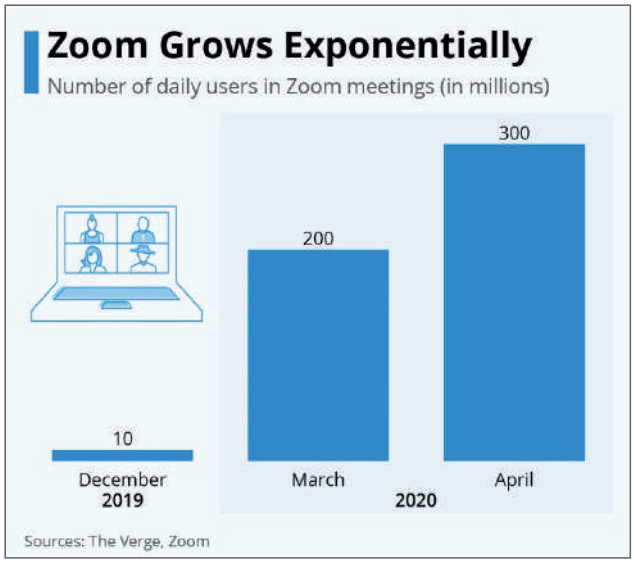
1] https://www.pwc.com/it/it/industries/fintech/docs/PwC-FinTech-2020.pdf

CYBERSEC
E DINTORNI

Zoom e Smart Working: cosa abbiamo imparato

Elena Vaciago
Associate Research Manager, The Innovation Group

Come noto sono stati numerosi i problemi di sicurezza incontrati da Zoom, la popolare app di web conference, passata da 10 milioni di utenti giornalieri a fine 2019 ai 200 milioni a fine marzo 2020 e a 300 milioni di utenti giornalieri a fine aprile. A fronte di un fatturato che ha toccato i 190 milioni di dollari nel quarto trimestre dell'anno fiscale 2020 (in crescita di 83 milioni di dollari rispetto al Q4 2019), il valore dell'azione è passato dai 76 dollari per azione del 31 gennaio ai 170 attuali.



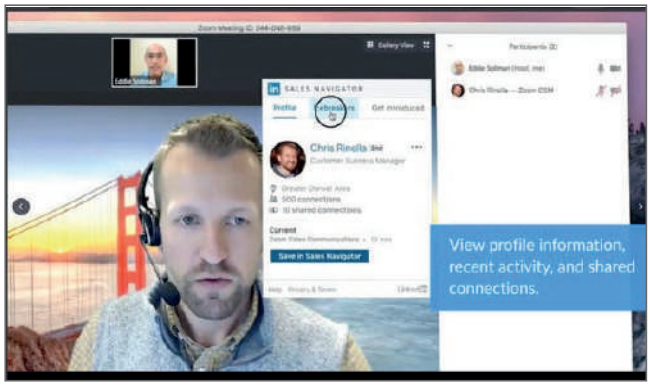
Ma Zoom è oggi anche sinonimo di cattiva gestione dei dati e mancanza di policy di sicurezza: mentre l'app veniva scaricata da milioni di persone, salendo tutte le classifiche e superando per numero di download anche le più popolari App social, l'azienda, alla rincorsa del successo, metteva infatti in secondo piano la sicurezza e incorreva in un'infinità di bug e procedure errate. Questo quello che è emerso:

- Scarsa attenzione alla privacy degli utenti:
  - Funzione (poi tolta) di "attendee tracking": chi organizzava un meeting poteva monitorare il livello di attenzione dei partecipanti a loro insaputa
  - Invio di informazioni sugli utenti a Facebook (anche per utenti NON registrati al social network)
  - Possibilità per i partecipanti (se iscritti al LinkedIn Sales Navigator) di accedere a informazioni LinkedIn di altri partecipanti a loro insaputa
  - Possibilità per sconosciuti (ma con lo stesso dominio, ad esempio, utenti di uno stesso ISP) di avviare call avendo visibilità completa dei contatti condivisi da Zoom (problema poi risolto).
- Mancate procedure di sicurezza:
  - Mancata crittografia end-to-end delle chiamate
  - A inizio aprile – di nuovo per una cattiva gestione interna – Zoom ha ammesso di aver "erroneamente" instradato alcuni dati degli utenti attraverso i server collocati in Cina.

- Vulnerabilità dell'app:
  - con la possibilità per gli attaccanti di installare l'app senza consenso degli utenti su MAC: in questo modo, se l'utente visita una pagina web compromessa, l'attaccante può attivare la sua telecamera e osservarlo (Apple è intervenuta disinstallando il software con una patch)
  - esposizione di credenziali Windows
  - possibilità di intercettare e inviare comandi ad un meeting in corso per persone che non partecipano alla riunione. Questo bug ha avuto grande clamore (in parte risolta, sono state fornite istruzioni su come configurare meglio il sistema per evitarla) in quanto ha permesso lo "Zoombombing", ossia, la possibilità per esterni di indovinare un Meeting ID e quindi potersi aggiungere in modo non protetto.

Ecco quindi coniato il nuovo termine, "Zoombombing", con cui si intendono azioni di disturbo organizzate che portano gli hacker a introdursi in videochiamate e riunioni a distanza. Aggressioni con insulti, minacce e molestie che ricordano molto quelle che negli ultimi anni si sono viste sui social network. Poi, ulteriori "accadimenti" sono stati:

- Furto di 500mila credenziali Zoom (nome utente e password), messi in vendita a un prezzo irrisorio, 0,002 centesimi di dollaro per un account (sembra però che potrebbero essere credenziali collegate ad altri data breach).
- Quasi contestualmente all'uscita della nuova versione di Zoom con la risoluzione di molti problemi di sicurezza (la 5.0), gli hacker "etici" di Morphisec Labs hanno individuato una nuova vulnerabilità dell'app che consentirebbe a un attaccante di registrare le riunioni e il testo delle chat a insaputa dei partecipanti ai meeting (anche se l'amministratore ha disabilitato l'opzione di registrazione).



Da notare che i vari problemi non sono emersi soltanto perché messi in luce dai ricercatori, ma spesso (come in un esperimento collettivo di cosa succede quanto si usa un software non sicuro) per le conseguenze reali che hanno avuto per moltissime persone: ad esempio, le situazioni con Zoombombing a un certo punto sono esplose in tutto il mondo, con interruzioni durante eventi culturali a distanza, incontri religiosi, corsi online, riunioni di amministrazione.

Tanto che lo stesso FBI ha rilasciato il 30 marzo un alert riportando il fatto di aver ricevuto moltissime segnalazioni da scuole del Massachusetts su intrusioni di troll con attacchi verbali di vario genere durante le lezioni.

Oggi, grazie anche all'arrivo dell'attesa versione 5.0 dell'app (annunciata con un post sul Blog ufficiale), molte problematiche di sicurezza sono state risolte.

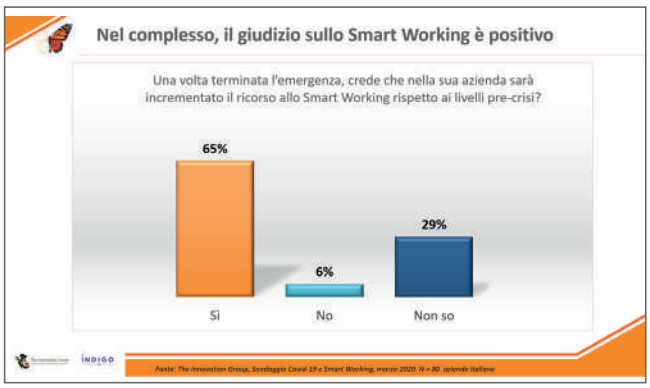
Ad esempio, l'azienda ha dichiarato che il problema di reindirizzamento (dati e conversazioni di utenti nordamericani con tanto di chiavi di cifratura sono stati inviare per sbaglio ad alcuni datacenter cinesi) è stato risolto il 3 aprile.

Altre misure di sicurezza introdotte sono le nuove policy per l'autenticazione e il collegamento di account, per il PIN della posta vocale, per gli accessi alle registrazioni effettuate (vulnerabilità che aveva portato a un breach relativo alle registrazioni), l'adozione della cifratura AES-256.

Vista la situazione, stupisce quindi che Zoom sia oggi così tanto utilizzato, ma il tema è che le riunioni online sono diventate negli ultimi due mesi molto frequenti, spesso indispensabili, per assicurare il lavoro o più in generale la socialità da remoto.

Cosa succedrà nella fase di ritorno alla normalità? In realtà, secondo molti avremo un proseguimento dell'utilizzo di questi strumenti. Secondo il sondaggio lanciato da The Innovation Group nella settimana del 25 marzo (subito dopo il Decreto del 24 marzo con cui venivano bloccate sia la circolazione delle persone sia moltissime attività), a cui hanno risposto 99 aziende dei diversi settori e con diversi ruoli, lo smart working è qui per restare: alla domanda se "Una volta terminata l'emergenza, crede che nella sua azienda sarà incrementato il ricorso allo Smart Working rispetto ai livelli pre-crisi?", il 65% delle persone ha risposto di Sì, il 29% non si è espresso, solo il 6% ha detto "No".

Motivo in più per stare attenti agli aspetti di sicurezza ….



CONNECTED MOBILITY

Il Contact Tracing per la ripresa della Mobilità

Elena Vaciago
Associate Research Manager, The Innovation Group

La ripresa delle attività e della mobilità delle persone nella fase 2 del post lockdown sarà facilitata dalla disponibilità dell'app nazionale di contact tracing.

In Italia, è stata scelta dal Governo l'app "Immuni" di Bending Spoons dopo una selezione su oltre 300 proposte pervenute.

Contact tracing con Immuni: cos'è, come funziona

Il contact tracing è da sempre uno dei migliori sistemi per prevenire il contagio da malattie infettive e quindi limitare la diffusione delle epidemie: è stato utilizzato in passato (con interviste dirette) per polio, HIV/AIDS, Ebola.

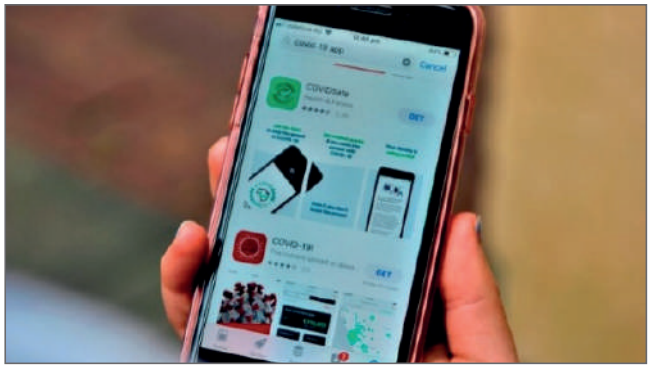
La tecnologia cellulare, oggi disponibile in gran parte della popolazione, rende più efficace il tracciamento, in quanto alcuni contatti potrebbero sfuggire alla memoria di chi viene intervistato, specialmente se, come nel caso del Covid-19, i giorni da considerare sono numerosi.

Inoltre, oggi nella maggior parte dei casi il contact tracing abilitato da Mobile utilizza la tecnologia di comunicazione Bluetooth, che funziona in vicinanza di una persona e quindi sembrerebbe perfetta a individuare un eventuale contagio con un virus che si propaga in prossimità di chi è infetto.

L'app Immuni scelta per l'Italia permette in sostanza di tenere traccia di tutte le persone con cui siamo entrati in contatto (per almeno 15 minuti, a una distanza tra 1 metro e 2 metri) nelle ultime settimane: se qualcuno di questi risulta poi infetto, veniamo avvisati, in modo che sia interrotta la catena del contagio tramite l'isolamento preventivo dei potenziali contagiati.

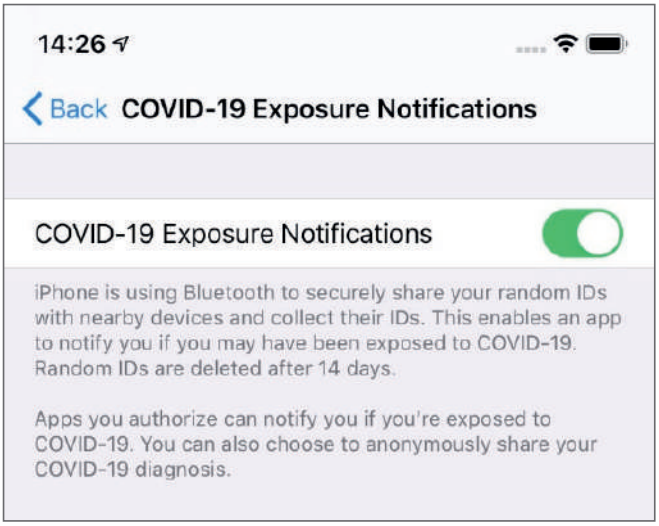
Esperienze internazionali, il caso dell'Australia

Tra le esperienze internazionali più interessanti di contact tracing abilitato da Mobile, quella già in corso in Australia con l'app COVIDSafe. L'app è sempre in esecuzione durante il giorno e quando si entra in contatto con altre persone. Le informazioni sono crittografate e l'identificatore crittografato viene archiviato in modo sicuro sul telefono (neanche l'utente vi può accedere). Le informazioni di contatto memorizzate nei cellulari delle persone sono eliminate (tenendo conto del periodo di incubazione Covid-19 e del tempo necessario per il test) in un ciclo continuo di 21 giorni. Quando alle persone viene diagnosticata la positività al virus, i funzionari sanitari chiedono a loro o ai loro genitori / tutori con chi sono stati in contatto. Se questi soggetti dispongono dell'app COVIDSafe e forniscono l'autorizzazione, le informazioni di contatto crittografate dall'app sono caricate su un sistema di archiviazione sicuro. A questo punto i funzionari sanitari utilizzano i contatti acquisiti dall'app per risalire ai contatti e chiamare le persone da avvisare, offrendo nel contempo consigli sui passi successivi (ad esempio, come e dove sottoporsi al tampone, fino a quali precauzioni adottare per proteggere amici e parenti da un'eventuale esposizione), il tutto senza mai nominare la persona risultata infetta. A dispetto di chi pensa che un'app del genere non piaccia alle persone, la COVIDsafe australiana, che è volontaria, in pochi giorni ha raggiunto 2 milioni di download.



A che punto siamo in Italia?

Nelle ultime settimane è sorto un vivace dibattito in merito alla scelta del sistema finale da utilizzare con l'app di contact tracing, se centralizzato (come vorrebbero Francia e Regno Unito), in cui la lista di tutti i codici identificativi degli smartphone delle persone con cui un utente è venuto in contatto sono gestiti su un server centrale, o di tipo decentralizzato (approccio scelto invece da Google e Apple) in cui tutti i codici sono gestiti a livello locale, e sul server centrale (collegato ai sistemi sanitari nazionali) sono registrati solo i dati legati agli smartphone delle persone contagiate. Il problema che si è verificato nelle scorse settimane è stato infatti che chi aveva scelto un approccio centralizzato, è incorso in inconvenienti tecnici, in quanto i sistemi operativi iOs e Android non assicuravano un funzionamento corretto. Inoltre, la soluzione di Google-Apple sarebbe più conforme ai dettami della privacy. Tutto questo ha probabilmente portato anche Bending Spoons (che inizialmente aveva sposato il modello centralizzato del progetto europeo progetto PEPP-PT) a propendere oggi per la soluzione DP-3T (modello decentralizzato) e all'utilizzo delle API di Google e Apple: con riferimento a quest'ultime, i 2 big tech hanno cominciato a fornire (il 29 aprile), ad alcuni sviluppatori, la versione Beta dell'aggiornamento dei propri software con l'Api di notifica delle esposizioni e l'Sdk collegato. Il rilascio definitivo delle API da parte di Google e Apple per le app nazionali di contact tracing è previsto a metà maggio.



Tutto questo fa pensare che sarà fine maggio il termine entro cui sarà disponibile a livello nazionale l'app di contact tracing. Ne avremo bisogno? Sicuramente sì, in quanto permetterà alle persone di muoversi più liberamente, con la possibilità di sapere se si è entrati in contatto con persone infette. Il diario clinico (sezione dell'app per colloquiare con il sistema sanitario) potrebbe però essere pronto più tardi, come ha detto il commissario per l'emergenza Domenico Arcuri.

Quali problemi ancora ne mettono in dubbio l'utilizzo?

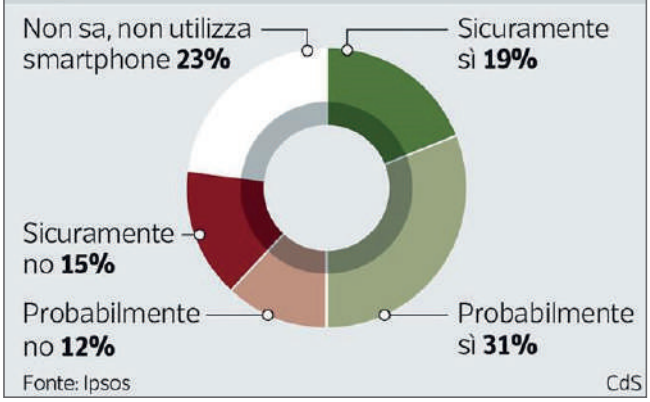
A parte i tempi legati allo sviluppo e all'operatività completa della soluzione, che appaiono piuttosto lunghi considerato anche il tema delle procedure sanitarie da preparare, il problema principale nel determinare il successo dell'app è legato a quanti ne faranno suo, perché il sistema è efficace se abbastanza diffuso.

In teoria, potrebbe fermare l'epidemia se usata dal 60% delle persone, mentre con numeri

di adozione inferiori potrebbe contribuire ad abbassare il numero dei casi ma non fermare i contagi, come ha spiegato Christophe Fraser, professore dell'Università di Oxford: "We've simulated coronavirus in a model city of 1 million inhabitants with a wide range of realistic epidemiological configurations to explore options for controlling transmission. Our results suggest a digital contact tracing app, if carefully implemented alongside other measures, has the potential to substantially reduce the number of new coronavirus cases, hospitalisations and ICU admissions. Our models show we can stop the epidemic if approximately 60% of the population use the app, and even with lower numbers of app users, we still estimate a reduction in the number of coronavirus cases and deaths." Ma non sappiamo con certezza se le app di contact tracing possono aiutare a ridurre la diffusione del contagio, perché non abbiamo informazioni certe in proposito: neanche in Corea del Sud (dove sono state impiegate ampiamente), erano soltanto un tassello del puzzle, e sono stati fatti moltissimi test per rilevare il prima possibile i positivi e isolarli dal resto della popolazione.

E comunque in Italia, secondo un recente sondaggio condotto da Ipsos, a dirsi disponibile a utilizzare Immuni è per ora solo una persona su due: il 19% scaricherà l'app sicuramente, il 31% probabilmente lo farà. A essere contrario all'idea di installare il software invece il 27%.

Lei pensa che scaricherà e utilizzerà l'app Immuni, quando sarà disponibile?



Fonte: Ipsos CdS

Altri problemi sono legati alla privacy e alla sicurezza delle applicazioni (in Italia, di questo si occuperanno il Copasir e il Garante Privacy), ma anche allo stesso funzionamento tecnico, che è tutto da verificare (Immuni sarà testata in un test pilota da 4mila dipendenti della Ferrari nei due stabilimenti di Modena e Maranello, sempre su base volontaria). In particolare, quanto e come dovrà funzionare il Bluetooth e considerando che la tecnologia ha un raggio d'azione ben superiore ai 2 metri (e può passare attraverso muri o barriere di protezione in plexiglass) come sarà evitato il problema dei falsi positivi.

DIRITTO ICT
IN PILLOLE

Data tracing: le Linee Guida dell'EDPB costituiranno le basi dei trattamenti futuri

Valentina Frediani
General Manager, Colin & Partners

Lo scorso 21 aprile il Comitato Europeo per la protezione dei dati ha emanato le Linee-guida 04/2020 sull'uso dei dati di localizzazione e degli strumenti per il tracciamento dei contatti nel contesto dell'emergenza legato al COVID-19.

Grande tema, oggetto di disamina, è il data–tracing: le linee-guida specificano condizioni e principi per l'uso proporzionato di dati di localizzazione e strumenti di tracciamento dei contatti.

In particolare, si fa riferimento all'utilizzo degli stessi per valutare l'efficacia complessiva delle misure di isolamento e quarantena adottate e da adottare.

Oltre a questo, viene considerato l'impiego del tracciamento dei contatti per informare chi possa aver stanziato in aree con soggetti a rischio al fine di poter interrompere la trasmissione stessa del contagio.

I punti fondamentali

Il Comitato ha indicato diversi punti che gli Stati Europei dovranno tener presenti sul tema data–tracing.

Misura fondamentale è quella dell'anonimizzazione dei dati relativi all'ubicazione dei cittadini, evidenziando come questi dati "anonimi" potrebbero in realtà non esserlo affatto.

Come si specifica nel testo: "le tracce di mobilità dei singoli individui sono caratterizzate intrinsecamente da forte correlazione e univocità.

Pertanto, in determinate circostanze possono essere vulnerabili ai tentativi di re-identificazione."

Inoltre, per quanto riguarda il principio della limitazione delle finalità, le stesse devono essere coerenti con gli obiettivi della gestione della crisi sanitaria, andando ad escludere categoricamente una raccolta dei dati per motivi ultronei.

Sul tema poi del data protection by design le indicazioni del Comitato sono estremamente nette in merito al funzionamento senza l'identificazione diretta delle persone, dovendo adottare misure che possano prevenire re–identificazione.

Inoltre, le informazioni raccolte devono rimanere allocate "fisicamente" nell'apparecchiatura terminale dell'utente a conferma della riduzione di ogni impatto ulteriore rispetto a quanto strettamente necessario.

Per quanto si possono conservare i dati?

Rispetto al principio di data retention quanto raccolto potrà essere conservato esclusivamente sino al perdurare della crisi legata al COVID–19; difficile, dunque, definire, in questa fase, una durata temporale specifica in considerazione delle variabili alle quali stiamo assistendo.

Mi preme evidenziare come il termine non sia ancorabile "allo stato di emergenza" citato nei nostri DPCM, bensì ad una più generica "crisi".

Questo elemento si pone dunque in un alveo di aleatorietà rispetto al tempo reale di mantenimento di attività dell'APP di tracciamento.

La sicurezza

Una misura di sicurezza dovrà essere quella relativa alla protezione dei dati con tecniche crittografiche di ultima generazione.

E, a proposito di misure di sicurezza, il Comitato ricorda l'obbligatorietà della produzione di una valutazione di impatto sulla protezione dei dati da condurre preventivamente alla implementazione della soluzione tecnologica alla luce del rischio connesso ai diritti dei cittadini, raccomandandone peraltro la pubblicazione.

Dunque, le Linee Guida – di cui abbiamo accennato solo alcuni dei punti più salienti – evidenziano come sia possibile un bilanciamento tra il diritto alla privacy dei cittadini e l'utilizzo di strumenti tecnologici che potrebbero condizionare positivamente i rischi legati alla salute delle persone.

Il precedente è creato?

Orbene, questo documento costituirà, per il futuro ormai prossimo, un punto di riferimento fondamentale laddove dovremo affrontare in generale, anche fuori dal momento pandemico, il tema del data–tracing.

Difatti, in un contesto epocale in cui assisteremo a cambiamenti radicali nella gestione dei flussi dati per finalità organizzative ed economiche (sia private che pubbliche) i principi di queste Linee Guida saranno di certo richiamati.

Esse hanno infatti focalizzato, rispetto al già esistente e consolidato Regolamento Europeo (GDPR) punti nodali rispetto a tecnologie legate ad intelligenza artificiale, industria 4.0 piuttosto che Internet of Things. Laddove citano, in modo molto dettagliato, il processo di tracciabilità pongono dei limiti validi anche per trattamenti diversi da quelli legati al COVID–19, indicando come, davanti alla inderogabilità legislativa connessa ad una pandemia, non si potrà mai derogare per finalità organizzative o di business.

Rileggiamo dunque le Linee Guida alla luce di questa riflessione, perché ciò implica, ed implicherà a chi commissiona o sviluppa applicativi che comportino tracciabilità, di valutare bene quanto i principi ivi dettati siano rispettati e come ciò sia dimostrabile in una ottica di accountability. Questo riguarderà integralmente il mercato europeo e tutte quelle società tecnologiche che sullo stesso intendano restare e competere.

VOCI
DAL MERCATO

Il crisis management nei giorni del covid-19

Intervista di **Elena Vaciago** a
Stefano Scoccianti
Enterprise Risk Manager, Gruppo Hera

Quali sono le strategie che le aziende devono attuare per contenere i rischi in caso di pandemia? Come riorganizzare il lavoro, a cosa prestare attenzione in ogni fase dell'emergenza, quali criticità tenere presente nel momento in cui la forza lavoro viene isolata e continua ad operare in autonomia da remoto? Ne abbiamo parlato con Stefano Scoccianti, Enterprise Risk Manager, Gruppo Hera.

Quali sono state per voi le misure fondamentali per contenere i rischi nel corso dell'emergenza creata dalla Pandemia Covid-19?

Nell'ultimo anno e mezzo nel gruppo Hera è stato avviato un processo di integrazione e ampliamento del modello di crisis management, un quadro di riferimento, dal punto di vista della governance e dei processi, per la gestione delle diverse categorie di crisi classiche (dall'interruzione di servizio, all'evento disastroso come un incendio, alla crisi di reputazione, per fare degli esempi), assegnando un ruolo centrale al Comitato di crisi. Questo è stato pensato a fronte di eventi che richiedono per rilevanza, intensità e strumenti di gestione, una focalizzazione specifica e straordinaria del gruppo e delle sue risorse, quindi attivabile quando l'evento travalica per importanza l'ambito circoscritto e gestibile a livello di singola attività di business. Il Comitato, che comprende il vertice aziendale e le figure chiave di importanti filiere aziendali, ha il compito di attivare i piani di gestione della crisi che, per capirci, vanno al di là degli ordinari piani di emergenza di cui le aziende e i loro impianti sono dotati. Nel caso della pandemia Covid-19, ci siamo trovati a gestire appunto una crisi non settoriale, non relativa ad un solo ambito del business, ma estesa a tutta l'organizzazione in tutte le sue componenti. Naturale quindi che andasse trovata una risposta trasversale e coerente per tutta l'azienda.

Abbiamo attivato fin dal 21 febbraio, quindi dalla scoperta del primo focolaio, un comitato tecnico che si è riunito costantemente nelle prime settimane, in modo da inquadrare e strutturare l'approccio di crisis management tenendo conto di due grandi ambiti di presidio e gestione dei rischi:

- Predisposizione di piani di continuità operativa, in coerenza con vari scenari evolutivi di severità della crisi individuati;
- Misure di prevenzione e protezione innovative per la safety delle risorse.

Abbiamo quindi strutturato piani di continuità operativa per gestire tutti i possibili scenari per tutte le filiere aziendali, cosicché quando c'è stato il lockdown generale non siamo stati colti impreparati. Sostanzialmente, in poco più di 1 settimana di lavoro, intenso, trasversale, abbiamo definito i piani di gestione, collegati alla situazione del momento ma tenendo anche conto di una possibile escalation della crisi e implementato molte delle misure di prevenzione e protezione.

Operativamente, è stato piuttosto impegnativo realizzare in tempi rapidissimi le misure di protezione per i dipendenti più esposti, come ad esempio le barriere in plexiglas per i colleghi che lavorano a contatto con il pubblico, negli sportelli a cui rivolgersi per i nostri servizi. Sempre per limitare il rischio di contagio tra i colleghi, abbiamo organizzato la sanificazione degli ambienti e diradato le presenze nelle mense, stabilendo distanze tra i posti e una turnazione per i pranzi.

Quali le misure in particolare per il lavoro da remoto?

Da metà marzo è partito anche questo aspetto. Prima ci eravamo concentrati su aspetti come turnazioni e segregazione logistica, squadre da dislocare su diversi luoghi di lavoro, in modo da ridurre la possibilità di contaminazioni tra diverse squadre, fino ad avere in campo (ad esempio per i telecontrolli) singole persone isolate dal resto dei colleghi. Vi era comunque già una quota di colleghi in modalità remote.

Poi, nel momento del lockdown generale, tale quota è cresciuta notevolmente rappresentando una percentuale elevata delle risorse non impegnate sul campo o in impianti, grazie all'utilizzo di collegamenti e tools adeguati. Questo è diventato nel corso delle settimane il nostro modo di lavorare, le comunicazioni sono state rese disponibili in ogni momento, mediante strumenti di condivisione e file in sharing. Dal punto di vista dell'IT, per garantire le attività in remoto, abbiamo velocizzato i processi di acquisto di PC portatili a fronte di una base disponibile già molto elevata, al fine di massimizzare le possibilità di lavoro da remoto per i colleghi (avendo scartato dall'inizio di consentire l'utilizzo del PC domestico privato).

Va detto che la situazione attuale, di remote working, ha trovato terreno fertile grazie alla preparazione effettuata negli anni precedenti da Hera nell'ambito del progetto di smart working rivolto a circa il 20% della forza lavoro.

Con l'emergenza Covid-19, è stato identificato e svolto un percorso per una popolazione significativa: sostanzialmente oggi le sedi si sono svuotate. Riguardo invece ai colleghi che si occupano di manutenzione (per definizione remotizzati) oggi, per evitare contatti diretti e

incrementare la sicurezza, la loro partenza avviene da casa (con il mezzo aziendale per l'intervento a disposizione sotto casa). Possono muoversi ed espletare la loro attività senza passare presso la sede, prendendo in carico l'intervento tramite tablet, senza bisogno di consegna fisica di ordinativi del lavoro da effettuare e quindi contatti diretti.

Si è parlato molto in questo periodo di rischi di filiera e di problematiche collegate alla Supply Chain nei giorni del Covid-19: qual è la sua esperienza su questo tema?

Considerando 3 ambiti di supply chain rilevanti in tale contesto (ICT, DPI e fornitori di servizi per le filiere di business), sulla parte ICT, essendo partiti per tempo e in gran parte già strutturati, non abbiamo registrato particolari criticità. Invece, come per molti altri, nell'ambito dei dispositivi di protezione ci sono state difficoltà: pur disponendo di nostre dotazioni di DPI, come strategia prudenziale abbiamo scelto di garantirci un livello di disponibilità adeguato alla situazione. Abbiamo dato corso ai contratti di fornitura esistente, pur nelle difficoltà e nelle incertezze di contesto, ed abbiamo anche attivato nuovi canali di fornitura grazie al nostro procurement.

Infine, sulla terza categoria di fornitura, ossia i partner locali sulle attività di esercizio, manutenzione, pronto intervento su reti e impianti, avendo partnership molto consolidate, abbiamo risolto le criticità che si presentavano tramite una maggiore cooperazione e coordinamento di tutti gli attori, operando nei limiti previsti dalle disposizioni normative che si sono susseguite.

Il nostro ufficio acquisti ha agito come osservatorio interno per valutare e individuare soluzioni per superare eventuali criticità per i vari cluster di fornitori, attivando ove possibile anche strumenti a sostegno della filiera. In questo momento non abbiamo segnali di criticità acute, ma c'è da dire che il nostro settore, essendo quello dei servizi essenziali, non è mai stato bloccato, e anche le catene di fornitura hanno continuato ad operare.

Cosa cambierà nei prossimi mesi?

Hera sta già predisponendosi per affrontare le settimane e i mesi che ci attendono, pur nelle incertezze riguardo alle modalità di ripartenza. Sicuramente una componente significativa sarà costituita dalle modalità di lavoro da remoto, componente importante per modulare il ritorno al new normal, e un ruolo rilevante sarà svolto dai vincoli che saranno imposti per il distanziamento sociale. La dotazione di mascherine potrà diventare un elemento chiave di protezione, così come prassi attivate in queste settimane lato sanitizzazione e igienizzazione. Potranno inoltre rendersi necessarie ulteriori misure per garantire livelli adeguati di sicurezza ai colleghi.

NOTE

NOTE

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...

CEDACRI GROUP

COMPILA IL FORM DI REGISTRAZIONE SU

www.theinnovationgroup.it