OTTOBRE 2023

IL CAFFÈ DIGITALE

THE INNOVATION GROUP NEWSLETTER

ITALIA DIGITALE

LE TAPPE E I SUCCESSI DELINEATI NELLA RECENTE NADEF

QUESTO MESE ABBIAMO FATTO COLAZIONE CON...

Francesco Di Maio
Gruppo Buffetti-Dylog

FOCUS PA

L'esempio del Nord-Est per la smart city digitale e sostenibile

METAVERSO

Metaverso, moda passeggera o futuro in evoluzione?

IL TEAM DEL CAFFÈ DIGITALE

Roberto MASIERO
Presidente
The Innovation Group

Ezio VIOLA
Co-founder
The Innovation Group

Emilio MANGO
General Manager
The Innovation Group

Elena VACIAGO
Associate Research Manager
The Innovation Group

Roberto BONINO
Giornalista, Research and Content Manager
The Innovation Group

Valentina BERNOCCO
Web and Content Editor
The Innovation Group

SOMMARIO

Italia digitale: le tappe e i successi delineati nella recente NADEF

Arianna Perri, Research Analyst
The Innovation Group

La transizione digitale è uno degli obiettivi di maggior rilievo per l'Europa, assumendo un ruolo centrale nell'ambito dei finanziamenti destinati dal Piano Nazionale di Ripresa e Resilienza (PNRR), riconoscendone la rilevanza strategica nell'innovazione e nella crescita economica del Paese

La Nota di Aggiornamento del Documento di Economia e Finanza (NADEF) recentemente pubblicata dal Governo italiano riserva un importante capitolo sulla digitalizzazione del Paese. Come ormai noto, la transizione digitale è uno degli obiettivi di maggior rilievo per l'Europa, assumendo un ruolo centrale nell'ambito dei finanziamenti destinati dal Piano Nazionale di Ripresa e Resilienza (PNRR), riconoscendone la rilevanza strategica nell'innovazione e nella crescita economica del Paese.

Nel documento vengono evidenziati i notevoli progressi compiuti dall'Italia che, nonostante partisse da una posizione arretrata, ha registrato sostanziali miglioramenti nei punteggi DESI negli ultimi cinque anni, grazie a una serie di investimenti mirati e un impegno politico sempre più incisivo nel campo digitale, sostenuto anche da un maggior afflusso di finanziamenti europei. Il PNRR assegna infatti il 25% del totale delle risorse per sostenere riforme e investimenti innovativi mirati alla digitalizzazione del Paese.

La Missione 1, in particolare, incentrata sulla "Digitalizzazione, innovazione, competitività, cultura e turismo", riveste un importante ruolo nel promuovere la transizione digitale nella Pubblica Amministrazione, in particolare attraverso il passaggio al cloud e l'interoperabilità dei sistemi informativi. La NADEF fornisce un dato concreto sull'avanzamento del passaggio al cloud: "sono state completate con successo la progettazione, preparazione, installazione e il testing di quattro data center, che costituiscono il nucleo di una nuova infrastruttura cloud, denominata 'Polo Strategico Nazionale' (PSN), dedicata a ospitare i sistemi informativi, i dati e le applicazioni di tutte le pubbliche amministrazioni. Nelle prossime fasi, si prevede la migrazione dei dataset e delle applicazioni di circa 280 pubbliche amministrazioni centrali e aziende".

Per quanto riguarda l'interoperabilità, è stata creata la Piattaforma Digitale Nazionali Dati (PDND), che consentirà l'interscambio di informazioni e servizi

tra enti semplificando e rendendo più efficienti procedimenti tradizionalmente complessi. Altro successo italiano è il raggiungimento degli obiettivi previsti per la diffusione di App IO e di PagoPa rispettivamente con due e tre anni di anticipo.

La digitalizzazione non riguarda però solo la Pubblica Amministrazione ma coinvolge anche la popolazione e la forza lavoro. L'Italia rimane infatti ancora sotto la media europea per quanto riguarda le competenze digitali di base dei cittadini, come sottolineato anche dal recente Report della Commissione Europea "2023 Digital Decade": i progressi circa le digital skill dei cittadini sono ancora piuttosto lenti e solo il 46% della popolazione possiede competenze digitali di base. Il suggerimento che viene dato all'Italia è di intensificare gli sforzi, con un particolare focus sul potenziamento delle competenze e sulla riqualificazione della forza lavoro. A tal proposito, come specificato all'interno della NADEF, il Governo ha adottato misure specifiche per migliorare le competenze digitali, con iniziative come la "Strategia nazionale per le competenze digitali" e il programma "Repubblica digitale". Entrambe le iniziative mirano a colmare il divario digitale tra l'Italia e gli altri paesi europei e prevedono il coinvolgimento di istituzioni pubbliche, istituti di istruzione e aziende, puntando a migliorare l'educazione digitale, sviluppare le competenze ICT specialistiche e promuovere la partecipazione dei cittadini alla vita democratica.

Il documento, inoltre, enfatizza come l'Italia stia lavorando per potenziare la catena di approvvigionamento dei semiconduttori, favorendo al contempo le transizioni verde e digitale. A tal fine, si sta finalizzando l'istituzione della Fondazione "Centroitaliano per il design dei circuiti integrati a semiconduttore" che "avrà il compito di promuovere la progettazione dei circuiti integrati, rafforzare il sistema di formazione professionale e favorire l'innovazione e il trasferimento tecnologico nel settore, anche partecipando a iniziative e programmi dell'Unione europea".

Come dichiarato nella NADEF, l'Italia sta investendo notevolmente sull'High Performance Computing (HPC): grazie a un investimento congiunto di 120 milioni è stato finanziato il supercomputer LEONARDO, inaugurato nel novembre 2022, attualmente uno dei più potenti al mondo.

Relativamente alla cybersecurity nel documento si legge: "Nell'ambito degli investimenti previsti per la terza rata del PNRR, l'attenzione si è focalizzata sulle misure in materia di cybersecurity. Dopo l'istituzione dell'Agenzia per la Cybersicurezza Nazionale, è stata avviata la definizione dell'architettura dell'ecosistema di cybersecurity nazionale; in questo ambito, saranno potenziati i sistemi di Cybersecurity delle PA locali e centrali".

I recenti progressi sulla migrazione in cloud

Grazie alla misura 1.2 del PNRR, con un finanziamento di 1 miliardo di euro, e alla grande partecipazione della PA locale ai bandi dedicati, è stato superato il target nazionale del Piano, che prevedeva la migrazione al cloud di 1.064 enti entro il 30 settembre 2023. Sono infatti ben 1.200 i Comuni e le Scuole che hanno migliorato i propri servizi digitali con il cloud.

L'implementazione del cloud sta portando, e porterà sempre di più, a una modernizzazione dei servizi digitali offerti, riducendo le code agli sportelli, ottimizzando la gestione amministrativa e didattica, semplificando i processi interni e migliorando l'efficienza delle amministrazioni locali.

In particolare, i Comuni hanno potenziato servizi fondamentali come la digitalizzazione degli atti e dei registri dello stato civile. Inoltre, l'adozione di strumenti digitali consente una condivisione più rapida e precisa delle informazioni demografiche con enti come l'Istat. La garanzia di sicurezza e affidabilità è stata assicurata grazie alle piattaforme cloud qualificate dall'Agenzia per la Cybersicurezza Nazionale (ACN).

Le Scuole, dall'altro lato, hanno migliorato la velocità e la precisione con cui vengono gestite informazioni cruciali come le presenze, gli esami e l'andamento didattico degli studenti, nonché i libri di testo e le votazioni finali. Inoltre, sono stati potenziati gli strumenti digitali per gestire in modo più efficiente l'economia, il personale e l'inventario, promuovendo una migliore pianificazione didattica e un ambiente scolastico più efficiente e all'avanguardia.

QUESTO MESE ABBIAMO FATTO COLAZIONE CON...

Francesco Di Maio
Direttore Cybersecurity di Gruppo Buffetti-Dylog

Zero Trust, dalla teoria alla pratica

Elena Vaciago, Research Manager
The Innovation Group

Il modello Zero Trust è un approccio alla sicurezza informatica che si basa sull'idea di non fidarsi implicitamente di nulla o di nessuno all'interno o all'esterno di un'organizzazione. In sostanza implica che nessuna parte, utente o dispositivo debba essere considerato automaticamente attendibile o degno di fiducia. Si basa su una serie di principi da seguire e ha l'obiettivo di ridurre al minimo il rischio di una violazione della sicurezza, oltre che di limitarne l'impatto, riducendo la superficie di attacco e controllando puntualmente gli accessi. Perché Zero Trust è oggi così importante? quali sono i suggerimenti per l'adozione? Ne parliamo in questa intervista con Francesco Di Maio, Direttore Cybersecurity di Gruppo Buffetti-Dylog.

Quali sono oggi i criteri alla base di una scelta Zero Trust, che è sempre più spesso suggerita anche dalle norme?

Quando perseguiamo una trasformazione digitale che non riguarda solo il mondo IT ma anche quello OT, in industrie che richiedono questi sviluppi, o ovunque si debba considerare il rischio legato alle terze parti, che sempre di più sono player implementativi principali o partner dell'azienda nell'esercizio, non si può prescindere dall'applicare logiche Zero Trust. Queste partono da un presupposto fondamentale, in particolare nella fase in cui le organizzazioni pubbliche e private non hanno più i tradizionali confini delle reti e dei sistemi on premises e diventa perciò indispensabile proteggere sempre di più l'informazione.

Oggi la dimensione del networking e la crescita dei dati è sempre più rapida e veloce, tanto che la stessa ACN, l'Agenzia di Cybersicurezza Nazionale, ha sentito la necessità di presidiare in maniera forte i processi del cloud, che diviene esso stesso centro di rilevanza per gli assetti strategici del Paese. Definita quindi la necessità di un modello Zero Trust, che necessariamente si basa su un approccio scalare e crescente, è però indispensabile svilupparne la sua attuazione in maniera sostenibile, comprendendone logiche di identificazione e considerando eventuali fattori che potrebbero impedirne lo sviluppo, a partire dalla necessità di un supporto convinto da parte dell'alta dirigenza.

Fin dall'inizio, quindi, fin da quanto si comincia ad approcciare in azienda il tema Zero Trust, è molto importante il supporto del vertice. Quali sono poi gli errori da evitare perché l'intero processo non si blocchi?

Ci dobbiamo interrogare su quali elementi possono rallentare l'adozione di politiche e logiche Zero Trust. Uno dei primi problemi risiede nella complessità dell'approccio stesso. Nessuno nega che iniziare un'implementazione Zero Trust sia veramente una rifondazione dei concetti fondamentali a partire dall'identità. Da sempre la gestione delle identità digitali si basa sui concetti dello IAM (Identity e Access Management) con un'evoluzione verso il PAM (Privileged Access Management): ci si è basati in passato su un criterio unitario. Oggi però, non lo si afferma mai abbastanza, abbiamo Zero Trust che non è semplicemente un prodotto che sostituisce uno precedente: si tratta invece di un modello organizzativo che tocca tutti, che comprende elementi sia legati alle persone sia alle tecnologie, con una forte componente di sviluppo culturale a tutti i livelli.

Il primo punto dell'adozione è quindi capire bene "cosa è Zero Trust".

A monte, è fondamentale. Anche perché, una domanda che uno potrebbe farsi è: "Quanto mi costa? E qual è il ritorno di un investimento così oneroso per un'attività che non ho ancora capito bene?" Abbiamo bisogno di un "evangelista di Zero Trust", con la capacità di far capire all'alta dirigenza, a CFO e altri dirigenti dell'organizzazione, sia essa pubblica o privata, che si tratta di un processo vitale, con costi d'implementazione iniziali

probabilmente notevoli, ma che nel medio e lungo periodo porta a una radicale modifica degli approcci di sicurezza ed una capacità di preservazione del patrimonio informativo che si ripaga nel tempo.

Prima o poi, dovremo tutti confrontarci con scelte diverse dall'uso di soluzione tradizionali on premises, avremo logiche di diffusione sempre più ampia dei dati del business, dovremo abbandonare la tradizionale protezione fisica di reti e hardware e passare alla protezione del dato in sé, elemento essenziale e critico per tutte le organizzazioni che oggi si confrontano con una notevole "esposizione tecnologica".

Un secondo aspetto critico, che indirizza la complessità d'implementazione di Zero Trust (ZT in seguito), è l'ancora perdurante esistenza di sistemi legacy. Le aziende hanno a livello infrastrutturale una stratificazione di oggetti, non sempre nati con logiche di security by design. Su questi, potrebbe risultare molto complesso applicare logiche di verifica e controllo ZT oriented. Il rischio potrebbe diventare quello di essere in grado di proteggere solo una parte dell'infrastruttura, qualcosa che alla fine vanifica gli sforzi fatti.

Un ulteriore problema è che affrontando ZT, inseriamo nella catena di produzione del business vincoli che possono risultare pesanti. Le persone spesso chiedono accesso alle informazioni, non voglio trovare vincoli, lacci e lacciuoli che rallentano il processo. La MFA, Multi Factor Authentication, ad esempio, è una tecnologia che, anche se spesso introdotta con fatica, comunque fa parte di una strategia complessiva che converge verso ZT. Quando si fa questa operazione su ambienti operativi della produzione, del business, si possono generare conflitti (come il rifiuto dell'utente di

essere identificato più volte), talvolta frutto di compromessi o di processi di ingegneria della security non agili e non sempre amichevoli verso l'esperienza dell'utente.

Questo elemento di complessità va superato, ancora una volta, con una virata culturale: oggi anche i produttori di sistemi che convergono verso ZT cercano di ridurre gli impatti sull'esperienza utente e questo richiede un'attenta valutazione iniziale dei requisiti, che sono il cuore di qualsiasi iniziativa progettuale, creando capitolati chiari, determinati, comprensibili, attuabili. Da una prospettiva diametralmente opposta, questo permette alle aziende, chiamate a confrontarsi sui bandi, di crescere e migliorarsi, creando una competizione di qualità.

Abbiamo poi, come ulteriore freno, il tema dei costi. Affrontare logiche ZT significa molto spesso ristrutturare completamente i processi IT di un'organizzazione. E questo è uno degli elementi più critici della logica di sviluppo di un processo ZT: quando abbiamo piccole imprese che hanno difficoltà a trovare risorse per implementare l'ordinario nell'IT, il problema diventa assolutamente serio.

Infine, deve essere chiaro che implementare ZT non assicura una completa sicurezza: la sicurezza assoluta, ricordiamolo, non esiste. Piuttosto, lo vedrei come elemento che compone un piano di cybersecurity più complesso, indirizzato sia alle minacce esterne, sia alle vulnerabilità interne.
In altri termini, se siamo tutti d'accordo che la sicurezza delle informazioni non si esaurisce solo su una specifica tecnologia, ma su attività organizzative, di processo e di fattore umano che si avvalgono di tecnologie abilitanti, è indispensabile tenere sempre a mente che la sicurezza delle informazioni è un'attività continuativa nella quale tutte le componenti vanno continuamente mantenute e aggiornate. Dall'altro lato, oggi per contrastare in modo efficace gli attaccanti, bisogna basare le attività di prevenzione e risposta su una Cyber threat intelligence intesa in senso evolutivo. Ossia, bisogna essere in grado di contrastare gli attori malevoli con la capacità di identificarne TTP (Tattiche, Tecniche e Procedure), ad esempio, utilizzando i processi di identificazione Mitre Att&ck ed automatizzando i processi di identificazione, per essere in grado di reagire velocemente: affiancando a questo la strategia ZT come elemento di prevenzione e di anticipazione della soglia di rilevamento, i livelli di sicurezza "di punto" e "di sistema" sono necessarialente destinati ad aumentare.

In conclusione, quali sono le tue raccomandazioni per l'introduzione di ZT in azienda e quali sono i benefici di questo modello per chi lo adotta?

È fondamentale far comprendere bene la filosofia ZT quale elemento privilegiato, attraverso il convinto supporto dell'alta direzione e delle strutture di business per ottenere una reale sicurezza del patrimonio informativo con benefici progressivi, molto evidenti nel medio e lungo periodo. Nella transizione da architetture tradizionali a modelli basati su cloud, il modello ZT risulta perfettamente allineato a questi obiettivi, e permette, proprio in sede di progettazione, economie di scala, efficienze di sistema, di applicare in maniera agile i criteri applicativi della strategia.

Ulteriori benefici nell'adozione di ZT è la gestione sicura della Supply chain. Oggi le organizzazioni, semplici o complesse che siano, devono far fronte a processi di interrelazione tra soggetti diversi, con modelli molto innovativi, ad esempio, di telecontrollo per la manutenzione degli apparati industriali o processi di outsourcing. Sono aspetti che devono tener conto di un'evoluzione ZT per contenere rischi emergenti anche di rilevante portata.

Un terzo e non marginale aspetto è l'opportunità di far crescere il mercato: è interesse di tutti che anche i fornitori di beni e servizi ICT intraprendano un percorso verso le logiche ZT, elemento di crescita professionale di qualità per il miglioramento complessivo della sicurezza cibernetica delle persone, delle imprese, delle organizzazioni, sia in termini di "security by design", sia nei processi di esercizio IT e di continuità operativa.

L'esempio del Nord-Est per la smart city digitale e sostenibile

Valentina Bernocco, Web and Content Editor
The Innovation Group

Padova si sta affermando come centro di sperimentazione e incubazione di startup, ma è anche una "Mission City" che si prepara per la neutralità climatica entro il 2023.

La casistica è tanto ampia da rendere difficile e forse poco sensata la ricerca di una definizione univoca. Tuttavia esiste una città italiana che può fungere da riferimento, da esempio di territorio che si trasforma per diventare sempre più tecnologico

Su quale sia, esattamente, la definizione di smart city il dibattito è aperto. Negli anni l'iniziale focus sulla digitalizzazione dei servizi (per esempio quelli di trasporto pubblico) si è allargato, e il concetto di "smart" si è sovrapposto all'idea di territori urbani più vivibili e anche ecologici, o se non altro meno grigi e inquinati. Gli sconvolgimenti della pandemia e dei lockdown hanno favorito la riflessione su nuovi modelli urbanistici e organizzativi, come l'ormai famosa concezione della "città in 15 minuti", teorizzata dall'urbanista Carlos Moreno. E in molti contesti, anziché parlare di smart city, si parla ormai di smart community, includendo nelle ambizioni di trasformazione anche le periferie e la provincia.

ma anche vivibile, sostenibile e (aspetto non secondario) attrattivo per i famigerati "talenti" alla ricerca di un'occupazione: Padova. Città storica di arte e cultura, è sicuramente più nota per gli affreschi di Giotto della Cappella degli Scrovegni o per la sua antica università (70mila matricole iscritte ogni anno, tra cui 6.500 stranieri) che non per l'innovazione digitale. Ma forse non tutti sanno che Padova è anche inclusa tra le 136 candidate nella Intelligent Cities Challenge, iniziativa della Commissione Europea per la transizione digitale, verde e socialmente responsabile dei territori urbani.

Merito anche della visione di Margherita Cera, giovane assessora del Comune di Padova che tra le sue molte deleghe ha anche quelle per Programma Agenda Digitale, Servizi Informatici e Telematici, Soft City. Ospite sul palco dell'Esprinet Tour (evento organizzato lo scorso 5 ottobre in collaborazione con The Innovation Group), Cera ha illustrato la visione di una "grande Padova", che trasforma non solo sé stessa ma funge da abilitatore per il territorio circostante, per aiutare i piccoli comuni nella trasformazione digitale. "La nostra città ha attratto mezzo miliardo di euro di risorse del Pnrr", ha detto Cera. "La forza di Padova è il suo legame con l'Università, che insieme alla Camera di Commercio, a fondazioni, banche, associazioni e acceleratori di startup ha creato un ecosistema dell'innovazione".

Questo ecosistema ha già prodotto risultati, come lo sviluppo di un "boulevard dell'innovazione", un asse stradale su cui si susseguono il centro congressi cittadino, un competence center dedicato all'industria 4.0, le sedi della Camera di Commercio, dell'Università, di Assindustria, centri i innovazione per startup (Le Village by Ca Triveneto e Paradigma), il parco tecnologico Galileo Visionary District e il centro di trasferimento tecnologico di M31. Non è un caso che, pur contando soli 200mila abitanti, il capoluogo veneto sforni più di un terzo dei brevetti registrati in Veneto: nel 2022 sono stati 679, il 34,5% del totale regionale.

Padova è anche una della cento "Mission City" selezionate dalla Commissione Europea (in base al lavoro già svolto e ai progetti presentati) per raggiungere la neutralità climatica nel 2030, con vent'anni di anticipo rispetto all'obiettivo fissato per le altre città europee. E sono già stati reclutati 38 stakeholder che sottoscriveranno un accordo per arrivare al "net zero" entro la fine del decennio. "La dimensione digitale dev'essere coordinata con tutte le iniziative riguardanti la sostenibilità", ha rimarcato Cera, "dunque anche con le piste ciclabili, con i mezzi pubblici e servizi di sharing. Ed è anche importante il collegamento con la piattaforma regionale MyData".

Quest'ultima è un'iniziativa regionale di raccolta e integrazione dei dati relativi a trasporto pubblico, viabilità, parcheggi e livelli di inquinamento, sostenuta con risorse del POR FESR 2014-2020 (Programma Operativo Regionali finanziato con Fondo Europeo di Sviluppo Regionale). Oltre 200 sensori e videocamere di proprietà municipale, più altri appartenenti ai privati, vengono utilizzati per creare mappe interattive e sempre aggiornate, che mostrano dati sul passaggio di mezzi motorizzati e biciclette. Il progetto è in fieri e includerà in futuro altre fonti di dati Internet of Things e funzioni di analytics.

La smart city è dunque una città che raccoglie e valorizza i propri dati al servizio del cittadino, della qualità dell'abitare e anche della sostenibilità. Inoltre è una città attrattiva per investitori, startup e professionisti alla ricerca di un ambiente imprenditoriale e lavorativo fecondo. Un'utopia? Per le grandi metropoli del mondo concretizzare questa visione è certamente complesso, e allora forse il compito di mostrare la vita spetta alle città più piccole e fortemente votate all'innovazione. Come Padova.

Via libera in Svizzera alla nuova Legge Federale sulla protezione dei dati: differenze e analogie con il GDPR

Yuri Monti, Consultant

Colin & Partners

Frutto di una profonda revisione della precedente legge sui dati personali, dal 1° settembre in Svizzera è entrata in vigore la nuova Legge federale sulla protezione dei dati (LPD). La nuova cornice normativa supera l'ordinamento del 1992, segnando un decisivo passo in avanti per i diritti dei cittadini in materia di trattamento e protezione dei dati personali. Una svolta necessaria, considerando la dirompente evoluzione tecnologica in termini di dispositivi e servizi che ha attraversato gli ultimi due decenni.

Ma vediamo cosa cambia rispetto al passato e soprattutto quali sono le affinità e le principali differenze della legge elvetica rispetto alla normativa europea in materia di protezione dei dati personali (GDPR). Aspetti, questi, di importanza centrale per i titolari del trattamento che abbiano relazioni dirette con la Svizzera e che pertanto devono prendere opportuna coscienza delle disposizioni previste dalla Legge federale.

Cosa cambia rispetto al passato

Le principali novità della nLPD – nuova Legge Federale sulla protezione dei dati – rispetto al precedente impianto sono:

1. La legge si applica solo ai dati delle persone fisiche non prendendo più in considerazione quelli delle persone giuridiche.
2. La definizione dei dati sensibili si estende anche alle categorie di dati genetici e biometrici.
3. Vengono introdottii principi di "Privacy by Design" e di "Privacy by Default", disponendo nell'ambito dell'art. 8 che titolari e responsabili garantiscano "appropriati provvedimenti tecnici e organizzativi".
4. In caso di rischio elevato per tutela delle persone e dei diritti fondamentali devono essere condotte delle analisi d'impatto, facendo propri gli adempimenti del GDPR connessi alla valutazione d'impatto (art. 22).
5. La raccolta di tutti i dati personali – non più soltanto di quelli sensibili – è subordinata all'obbligo di informare preventivamente gli interessati.
6. Viene introdotto, a determinate condizioni, l'obbligo di dotarsi di un registro dei trattamenti e la facoltà di nominare un "consulente per la protezione dei dati" (figura analoga a quella del DPO prevista dal GDPR).
7. In caso di violazione dei dati personali, il titolare deve notificare il breach all'Incaricato federale per la protezione dei dati e per la trasparenza (IDT), ovvero il Garante svizzero, eccetto non si tratti di uno dei casi per cui tale obbligo non sia previsto.

8. Introduzione della nozione di profilazione (inteso come trattamento automatizzato dei dati personali) che nella normativa svizzera prevede un'accezione peculiare con la definizione di "profilazione a rischio elevato", ossia "che comporta un rischio elevato per la personalità o i diritti fondamentali della persona interessata".

LPD e GDPR a confronto

Da un primo sguardo emergono chiaramente le somiglianze con il General Data Protection Regulation e come molti dei principi ed istituti applicabili al trattamento di dati personali in Svizzera siano mutuati – in maniera più o meno pedissequa – dal Regolamento Europeo. Lo si nota in maniera evidente nelle stesse definizioni "dati personali" e "interessato" con significati analoghi a quelli tracciati dal GDPR o di "dati personali degni di particolare protezione" praticamente sovrapponibile con la versione europea di "categorie particolari di dati personali".

Stesso livello di analogia è riscontrabile sia negli obblighi informativi a capo dei titolari che nei diritti nei confronti degli interessati. Non meno rilevante il tema del trasferimento di dati personali all'estero per cui si rendono necessarie adeguate garanzie e deroghe come novellato al Capo V del GDPR.

L'impatto della nuova cornice normativa non avrà effetti dirompenti per le imprese elvetiche e non che avevano già affrontato il processo di adeguamento al GDPR e che potranno godere di un indubbio vantaggio sia in termini tecnici e organizzativi che a livello competitivo rispetto al mercato. Non meno trascurabile l'aspetto connesso all'ambito di applicazione: la LPD, infatti, si applicherà "alle fattispecie che generano effetti in Svizzera, anche se si verificano all'estero"; ciò significa che – sebbene tale interpretazione non sia ancora confermata da pronunce e/o provvedimenti del Garante svizzero – ogni qualvolta un titolare del trattamento si trovi a trattare dati personali di cittadini svizzeri, è soggetto al rispetto del suddetto impianto normativo.

Ulteriore punto su cui merita soffermarsi è quello descritto all'articolo 14 relativo alla possibile necessità di nominare un rappresentante in Svizzera. Non si tratta di una riproposizione dell'art. 27 del GDPR, ma vi è una sostanziale differenza nelle indicazioni dell'art. 14 della LPD: nel testo si legge infatti che qualsiasi titolare che, pur avendo sede all'estero, tratti dati personali di cittadini svizzeri debba nominare un rappresentate in Svizzera nel caso in cui (i) il trattamento sia connesso "a un'offerta di merci o prestazioni o finalizzato a porre sotto osservazione il comportamento di dette persone", (ii) sia un trattamento su larga scala, (iii) sia un trattamento periodico e (iv) comporti un rischio elevato per la personalità delle persone interessate.

Rispetto alla normativa GDPR, quella elvetica, pur imponendo al titolare di affidare il trattamento ad un responsabile in grado di garantire la sicurezza dei dati personali, non ne definisce le modalità e non approfondisce diritti e doveri che ne disciplinano il rapporto con il titolare, come invece avviene dettagliatamente e in maniera molto strutturata nel Regolamento europeo (art. 28 GDPR).

Sul fronte sanzionatorio – per concludere questa breve analisi – la Legge Federale prevede, in caso di violazione delle disposizioni, sanzioni, per la persona fisica, fino ad un massimo di 250.000 franchi. Nel caso in cui le persone fisiche responsabili delle violazioni non siano ragionevolmente individuabili e la multa non superi i 50.000 franchi, le sanzioni potranno ricadere direttamente sulle aziende.

METAVERSO

Metaverso, moda passeggera o futuro in evoluzione?

Arianna Perri, Research Analyst
The Innovation Group

Negli ultimi anni, il concetto di metaverso ha guadagnato terreno nell'immaginario collettivo, diventando un tema centrale nelle discussioni sul futuro della tecnologia e sulla trasformazione della società. Ma cosa si cela dietro questa parola tanto discussa? E cosa significa per il futuro della nostra identità digitale e delle generazioni a venire?

Sebbene il concetto di metaverso non sia una novità, avendo avuto origine nel 1992 nel mondo cyberpunk, la sua diffusione nella cultura popolare è diventata evidente con l'annuncio di Facebook di cambiare nome in Meta nell'ottobre 2021, con l'obiettivo di focalizzare gli investimenti e gli sforzi sulla creazione di un metaverso. A tre anni di distanza dall'annuncio di Meta e dalle molteplici ipotesi, previsioni e speculazioni sul suo futuro, ci chiediamo: a che punto siamo? Basandoci sulle stime della società di consulenza McKinsey il metaverso non è solo una parola di moda, ma una realtà sempre più concreta: entro il 2030 il mercato del metaverso arriverà a valere 5 trilioni di dollari, influenzando diversi settori, dal B2B al B2C. Uno dei settori maggiormente interessati sarà l'e-commerce, con previsioni che indicano un impatto compreso tra i 2 e i 2,6 trilioni di dollari entro il 2023.

Secondo i detrattori, al contrario, il termine metaverso appartiene al passato, ed è considerato persino "scomodo" da utilizzare. Nonostante ciò, molti stanno osservando da vicino le evoluzioni di questo trend tecnologico, come dimostra l'ampia partecipazione al "Festival del Metaverso", un evento interamente dedicato all'ecosistema metaverso organizzato dall'Associazione Nazionale Giovani Innovatori (ANGI) e tenutosi a Torino lo scorso 10 ottobre.

Metaverso e imprese, quali possibili applicazioni?

Durante il Festival, gli interventi hanno dimostrato che il metaverso oggi è sempre più concreto, soprattutto se abbinato ad altre tecnologie emergenti: Generative AI, Blockchain, Machine Learning, Extended Reality, eccetera. Le aziende stanno dunque iniziando a comprendere il reale potenziale del metaverso, la cui evoluzione sta gradualmente superando la sua iniziale connotazione legata esclusivamente al mondo del gaming. Come testimoniato dai contenuti degli interventi durante l'evento, le applicazioni sono molte e nei più svariati settori:

- Marketing e comunicazione: campagne pubblicitarie immersive e interattive, esposizioni virtuali di prodotti e servizi.

- Sanità: soluzioni per facilitare le attività riabilitative, simulazioni di interventi chirurgici, terapie virtuali e consulenze mediche a distanza.
- Turismo: esperienze virtuali di viaggio, visite guidate virtuali a luoghi turistici e culturali.
- Collaborazione in azienda: uffici virtuali, riunioni e team building in ambienti digitali condivisi.
- Formazione e istruzione: corsi virtuali interattivi, laboratori pratici simulati e lezioni immersive.
- Intrattenimento e cultura: visite ai musei, cinema, eventi e concerti virtuali.
- Gaming: giochi multiplayer immersivi.
- Non profit e sociale: esperienze immersive di sensibilizzazione, su tematiche quali, ad esempio, il cyberbullismo.
- Sport: eventi sportivi virtuali, addestramenti e simulazioni di competizioni, coinvolgimento degli appassionati attraverso esperienze immersive.

Secondo una recente ricerca condotta da EY e Nokia su un campione composto da 860 dirigenti aziendali, tra le aziende che prevedono di investire nel metaverso in futuro, il 58% ha già intrapreso questo percorso e ha avviato almeno un caso d'uso nella propria organizzazione. Solamente il 2% del campione considera il metaverso una tendenza passeggera, dimostrando un forte consenso sulla sua rilevanza a lungo termine. Anche tra le aziende che finora non hanno intrapreso alcun percorso in questo campo, il 94% prevede di avviare i primi progetti entro i prossimi 24 mesi, sottolineando il crescente interesse e l'urgenza di adottare il metaverso come parte integrante delle strategie aziendali.

L'opinione dei cittadini-utenti sul metaverso

Una recente indagine condotta da Lab21.01 su un campione di 1.000 giovani under 35 e presentata in anteprima nel corso dell'evento, ha messo in evidenza le principali tendenze riguardanti la percezione del concetto di metaverso. A distanza di un anno dalla prima rilevazione, sono emersi segnali positivi riguardo alla conoscenza del termine e alla sua influenza. In particolare, il 35% del campione si dichiara consapevole del significato del termine metaverso: la prima associazione che scatta nella mente dei giovani italiani quando si parla di metaverso è un universo virtuale, aumentato e parallelo, con il 60% delle risposte, seguita dalla fusione tra un videogioco e il mondo reale (26%) e dal semplice videogioco (14%). Il 31% del campione dichiara

inoltre che il metaverso impatterà principalmente il settore dell'istruzione e della formazione (31%) e della mobilità, turismo e smart city (24%); l'e-commerce viene indicato invece solo dall'11% dei giovani intervistati.

Nonostante la crescente consapevolezza, solo una minoranza ha sperimentato un'esperienza immersiva nel metaverso (9%), mentre la stragrande maggioranza degli intervistati dichiara di volerlo fare (72%), con una piccola quota (11%) che manifesta opposizione. Quando viene chiesto di immaginare in che modo il metaverso rivoluzionerà la società, i giovani italiani indicano la possibilità di abbattere le distanze sociali (29%) come cambiamento più significativo, seguito dall'incremento di spazi e strumenti tecnologici (21%), l'opportunità di creare un ambiente di gender and age equality (19%), nuove possibilità di lavoro (17%) e la creazione di nuove identità (14%).

Non è tutto oro quel che luccica: le criticità

Non è un segreto che ad oggi la tecnologia non sia ancora del tutto matura: i visori, ad esempio, che rappresentano l'unica chiave per un'esperienza immersiva nel metaverso, non hanno ancora raggiunto il loro pieno potenziale. In questo contesto, Apple ha annunciato l'uscita del suo nuovo visore, Apple Vision Pro, a partire dal 2024, inizialmente sul mercato statunitense. È curioso notare che Apple, nelle sue comunicazioni, non menzioni il metaverso, riferendosi bensì al concetto di Spatial Computing, un termine ancora poco conosciuto ma che potrebbe rivelarsi altrettanto importante, se non di più, rispetto al metaverso.

Le ultime notizie, inoltre, non promettono bene per il futuro del metaverso: Meta continua a registrare importati perdite operative nella divisione Reality Labs, seppur previste nel piano aziendale, mentre Disney, Tencent e Snapchat hanno sciolto la propria unità dedicata al metaverso. Anche la Commissione Europea, circa un anno fa, date le poche adesioni, ha "chiuso" il suo metaverso, costato 387mila euro.

Un punto fermo emerso durante il "Festival del Metaverso" è che questo rappresenta sicuramente una nuova dimensione, un nuovo "non luogo", nel quale però, noi, ci muoviamo non più come individui fisici, ma come dati in costante movimento. In questa dimensione l'essere umano è stato trasformato in un "dato", un'entità digitale in un mondo virtuale in continua evoluzione. Questa trasformazione ci costringe a riflettere su una criticità derivante dalla diffusione di questa – e non solo – tecnologia: come proteggere, gestire e comprendere la nostra identità digitale. Investire nella sicurezza informatica da sola non è sufficiente; la soluzione è mantenere la persona al centro: il metaverso crescerà, infatti, anche in funzione dell'aumento di consapevolezza e senso critico delle persone. Un'altra sfida importante riguarda la formazione delle nuove generazioni alle tecnologie emergenti: prima ancora di pensare a nuove regolamentazioni, la vera rivoluzione inizia dall'educazione.

Il metaverso offre un'ampia gamma di opportunità, dalla riduzione dei costi dei trasporti all'aumento dell'efficienza e alla stimolazione delle relazioni sociali, sebbene sia ancora in fase evolutiva e presenti sfide come la standardizzazione dei dispositivi. Il concetto stesso di metaverso è in costante evoluzione, ed è ora più ampio: spesso viene utilizzato per indicare esperienze di realtà aumentata (Augmented Reality) o realtà estesa (Extended Reality), e abbraccia molte tecnologie abilitanti: dalla Blockchain, agli NFT, all'internet delle cose. Oggi va anche considerato l'impatto su questo mondo, per la grande popolarità raggiunta in brevissimo tempo, dell'AI generativa.

In questo contesto di rapido cambiamento, il ruolo delle persone è fondamentale: siamo noi a guidare il cambiamento, a plasmare il metaverso e trasformarlo in opportunità.

Il metaverso offre un'ampia gamma di opportunità, dalla riduzione dei costi dei trasporti all'aumento dell'efficienza e alla stimolazione delle relazioni sociali, sebbene sia ancora in fase evolutiva e presenti sfide come la standardizzazione dei dispositivi.

L'inflazione si può combattere con l'agilità?

Roberto Bonino, Research and Content Manager
The Innovation Group

Il tema dell'inflazione riguarda tutti noi per gli effetti sui prezzi, quindi anche le funzioni aziendali e fra queste l'It. L'aumento dei costi incide sulle decisioni da prendere e sulla definizione dei budget, che però devono fari i conti anche con i progetti di trasformazione digitale, le evoluzioni delle infrastrutture e la protezione dalle crescenti minacce cyber. Secondo l'opinione di analisti e integratori, l'agilità e l'adattabilità possono essere le chiavi di una gestione ottimale dei sistemi informativi in tempi turbolenti.

In questi ultimi anni, molte aziende hanno dato priorità alla digitalizzazione, destinandovi quote importanti di budget. Oggi però la crescente domanda di servizi It sta facendo aumentare i costi, sotto l'effetto di fattori come l'inflazione globale o l'espansione degli hyperscaler. I costi energetici o quelli delle risorse (interne o esterne che siano) hanno un'incidenza diretta sull'economicità dell'It, ma anche chi ha fatto la scelta del cloud

> **Per ragioni idealmente economiche, le imprese hanno optato in questi ultimi anni per l'adozione di metodologie agili e per la migrazione di dati e processi verso il cloud soprattutto pubblico**

deve confrontarsi con aumenti imposti anche dai grandi provider come Microsoft (11% annunciato nello scorso aprile) o Google (addirittura il 50% sullo storage).

Semplificando un po', si può dire che oggi le spese tecnologiche possono dipendere da scelte architetturali o da imperativi dettati dalla cybersecurity. Per ragioni idealmente economiche, le imprese hanno optato in questi ultimi anni per l'adozione di metodologie agili e per la migrazione di dati e processi verso il cloud soprattutto pubblico. Tuttavia, se nel momento della decisione lo scenario poteva apparire conveniente, molti hanno dovuto constatare un aumento dei costi nel medio termine. Il motivo principale è che il volume dei dati trattati è andato aumentando in modo molto rapido, così come i comportamenti delle applicazioni e la gestione dei portafogli hanno bisogno di risorse informatiche in costante evoluzione.

La migrazione dei dati e dei workload verso il cloud pubblico, un'architettura ibrida o multicloud può rivelarsi una soluzione anche economica e sicura, a patto che sia associata a una trasformazione strategica. Quali sono le reali necessità di storage? Come conservare e per quanto i dati?

Quali sono i costi di manutenzione? Come strutturare i dati e utilizzare i container? Come evitare la moltiplicazione dei dati e la loro ridondanza? Cosa portare in cloud e cosa lasciare in-house? La risposta a queste domande dovrebbe essere la base per definire una griglia di costi a breve, medio e lungo termine.

Le testimonianze che raccogliamo nei nostri eventi e nelle conversazioni con i Cio delle aziende fanno intendere che l'agilità, affiancata a una innovazione equilibrata, sono i fattori che meglio consentono di adattarsi anche alle fluttuazioni economiche. Per i Cio la questione centrale riguarda l'equilibrio fra bisogni e implementazione di un sistema efficace, la sicurezza informatica e la gestione dei costi. In un contesti di incertezza, appare preferibile privilegiare soluzioni che si basino sull' architettura per stabilire un modello affidabile e duraturo, che possa essere controllato e ottimizzato.

Mantenere una prospettiva sull'intera strategia It implica anche identificare i partner giusti. Dato che le soluzioni It si evolvono rapidamente, è, ad esempio, difficile disporre di tutte le competenze internamente. Valorizzare professioni a valore aggiunto per l'azienda, come quelle dei data analyst piuttosto che internalizzare le competenze in ambienti container appare un approccio più strategico. Infine, va attentamente monitorata anche la dimensione contrattuale: se da un lato è opportuno privilegiare i fornitori che propongono accordi pluriennali con prezzi decrescenti, dall'altro è necessario restare vigili sulle condizioni di uscita per non ritrovarsi interamente legati a un unico player.

Il valore della cybersecurity percepito dal business

Stefano Scoccianti

Enterprise Risk Manager, Gruppo Hera
Consigliere ANRA

La cybersecurity ha oggi acquisito un'accentuata visibilità nel contesto aziendale per le conseguenze delle crescenti minacce informatiche, per le iniziative legislative europee e nazionali volte a migliorare la cybersicurezza aziendale, e in generale per la comune esperienza dei responsabili di funzioni e attività aziendali. A fronte di una sempre più diffusa percezione della rilevanza della sicurezza informatica, vi sono tuttavia diversi gradi di consapevolezza all'interno delle realtà imprenditoriali, conseguenza del valore percepito della cybersecurity correlato alle industry di appartenenza, alla natura dei sistemi informatici prevalenti, alle funzioni aziendali di appartenenza. A titolo esemplificativo, aziende impegnate nell'erogazione di servizi essenziali e aziende venditrici di servizi a mercato possono presentare profili di valore percepito delle tematiche cyber diversificati in relazione alla consapevolezza delle conseguenze indotte da eventi avversi.

I soggetti che operano facendo ampio ricorso ad ambienti OT (Operation Technology)

gestiscono attività per le quali è necessario garantire continuità dei processi produttivi e dei servizi, in particolare nel caso di servizi pubblici essenziali. Vi è chiara percezione dell'importanza dei sistemi di monitoraggio e gestione di infrastrutture, impianti, linee di produzione, reti e delle conseguenze di un loro improprio funzionamento o indisponibilità. La protezione di tali asset, la capacità di intercettare anomalie, la prontezza di intervento in caso di rilevazione di comportamenti fuori standard, sono in genere adeguatamente apprezzati e sollecitati dal management.

Analoga importanza viene attribuita alla sicurezza degli ambienti IT (Information Technology), i sistemi informativi utilizzati nei processi transazionali di business, siano essi di natura amministrativa o a servizio della customer experience. Anche per tali sistemi vi è un evidente ed esplicito valore percepito da parte del business: se ad esempio i canali digital di contatto, vendita e gestione dei clienti sono indisponibili per un attacco hacker, rendendo inutilizzabile la piattaforma gestionale a supporto, si riducono le opportunità di business e soprattutto aumenta la pressione sui canali fisici alternativi, non sempre in grado di assicurare il medesimo livello di servizio. Le conseguenze derivano anche dal maggiore costo di processamento e gestione delle procedure commerciali e amministrative. Sono inoltre facilmente intuibili le potenziali conseguenze sul piano reputazionale connesse alla percezione di affidabilità dell'azienda stessa.

Un'area in cui il valore percepito della sicurezza cyber da parte del business non è talora in linea con la sua rilevanza è costituita dai rischi di compliance della protezione dei dati (GDPR). Le conseguenze derivanti dalla mancata adesione agli standard previsti dalle norme possono determinare, oltre agli oneri per il ripristino a seguito di un data breach, anche sanzioni irrogate dalle autorità di settore e impatti reputazionali che mettono a dura prova il ruolo dell'azienda quali partner affidabile del cliente. La mancata esperienza di eventi di tale natura e l'apparente intangibilità dell'impatto

reputazionale rendono il business talora meno sensibile a tale rischio specifico.

Il CISO (Chief Information Security Officer) è una figura organizzativa chiave nel rendere percepibile il valore del cyber risk, favorendo l'accrescimento della sensibilità aziendale alla gestione dei rischi cyber e la promozione della cultura della sicurezza. Non è tuttavia sufficiente la sua presenza se manca l'articolazione della governance a supporto della sua attività. È fondamentale cioè che sia definito l'insieme delle politiche, delle procedure e dei processi per gestire e monitorare i rischi attraverso le opportune leve aziendali a garanzia degli obiettivi di business.

L'approccio più efficace prevede che il CISO/DPO incanali la governance dei rischi gestiti in quella più ampia dei rischi di gruppo o, ove essa sia assente, la solleciti. A sua volta la governance dei rischi diviene parte del Risk Appetite Framework (RAF) aziendale, ovvero dell'insieme dei criteri che consentono di definire e gestire il profilo di rischio aziendale, identificando

- le responsabilità, ovvero chi ha le leve per fare cosa, distinguendo tra chi valuta e indirizza la strategia di resilienza e chi la mette in atto (action owner)
- i processi di gestione, ovvero come si affrontano i rischi, inclusa la gestione incident, l'escalation e il recovery
- l'infrastruttura di supporto attraverso cui si fa la gestione, sia essa materiale (risorse economiche e tecnologiche) che immateriale (metodologie e risorse umane)

Un'ultima considerazione connessa al tema del valore della sicurezza riguarda l'importanza della comunicazione aziendale. È possibile identificare tre tipi di comunicazione afferenti ai rischi e nello specifico alla cybersecurity

- le comunicazioni tecniche e l'interlocuzione con organismi esterni di settore, diretta responsabilità del CISO/DPO
- le comunicazioni esterne non tecniche, da sviluppare con il giusto accento e le appropriate modalità, verso i media, i clienti, le istituzioni non di settore, che sono svolte sia in forma preventiva, consolidando la percezione di presidio e affidabilità dell'azienda sulle tematiche in questione, sia in caso di emergenza, la cui responsabilità è di solito attribuita alla funzione istituzionale di comunicazione
- le comunicazioni interne non tecniche verso l'universo di soggetti non specialisti del rischio, per valorizzare anche il loro contributo alla sicurezza aziendale e assicurare un'adeguata formazione e diffusione della cultura del rischio, accrescendo al contempo il valore percepito dai colleghi verso tali iniziative

È bene che le tre tipologie di comunicazione, pur nella distinzione di linguaggio, contenuti, destinatari e tempistiche, siano coerenti e seppur finalizzate al loro scopo specifico, contribuiscano a rendere evidente il valore della sicurezza informatica.

ISCRIVITI ALLA NEWSLETTER MENSILE!

Ricevi gli articoli degli analisti di The Innovation Group e resta aggiornato sui temi del mercato digitale in Italia!

COMPILA IL FORM DI REGISTRAZIONE SU

www.theinnovationgroup.it