

## DigitEconomy.24 – IL CLOUD E I PROBLEMI DI CYBERSECURITY

L'INTERVISTA AL PRESIDENTE DEL COMITATO PARLAMENTARE PER LA SICUREZZA DELLA REPUBBLICA

# Urso (Copasir): «Su dati e rete a banda larga va definita la strategia nazionale»

**S**ulla cybersicurezza, uno dei grandi problemi che si porranno a livello globale, «dobbiamo fare in fretta e fare bene». È la posizione di Adolfo Urso, presidente del Copasir, alla luce dell'evoluzione delle tecnologie e dell'esigenza di tutela dei dati dagli attacchi informatici. Proprio nel campo dei dati, «si ridisegneranno gli assetti globali». Il cloud nazionale, la strategia sulla rete a banda larga, «che va definita», le interconnessioni attraverso i cavi marittimi nel Mediterraneo, lo sviluppo tecnologico e produttivo sui chip e sui semiconduttori, le batterie elettriche e ovviamente l'intelligenza artificiale «sono elementi importanti di quella che deve essere una chiara e definita strategia nazionale, condivisa con i nostri partner europei e atlantici». **Ad agosto è stata approvata la legge**



↑ **Adolfo Urso**,  
presidente del Copasir

**sulla cybersicurezza che prevede anche la nascita dell'Agenzia ad hoc. Si può dire che l'Italia ha oggi uno scudo sufficiente per proteggersi dagli attacchi?**

L'agenzia sta muovendo i primi passi e mi auguro che possa presto essere in piena attività. La sua realizzazione giunge con qualche anno di ritardo rispetto ad altri Paesi europei, anche se nel frattempo, grazie proprio alla

### DRAGHI: «ASPETTIAMO LE OFFERTE PER IL CLOUD»

Si scaldano i motori per il polo strategico nazionale del cloud della Pubblica amministrazione. In occasione dell'assemblea di Confindustria, anche il presidente del Consiglio, Mario Draghi, ha ricordato la strategicità del progetto: «attendiamo di ricevere le prime proposte di partnership per il polo strategico nazionale». Un tema per cui «sarà importante il contributo dei privati». Per il presidente di Asstel, Massimo Sarmi, «si è acquisita la consape-



volezza del valore dei dati sia in termini di sicurezza sia di generazione di ricchezza; ora si tratta di trovare la formula, le competenze ci sono, l'impianto sarà fatto sicuramente».

attività, che potremmo definire di supplenza, della intelligence e all'impulso del Copasir sono stati realizzati altri tasselli importanti, per esempio il peri-

>> continua a pag. 2

### PARLA IL COUNTRY MANAGER ITALIA DI ORACLE

## «Pronti a partecipare al cloud nazionale, a breve la nuova region cloud»

«**S**iamo ben posizionati a tutti i livelli e con tutte le aziende per far parte del progetto di cloud nazionale». Oracle Italia, società che è nel nostro Paese da 40 anni e conta 1.100 dipendenti, si candida a far la sua parte per il progetto annunciato dal ministro dell'Innovazione tecnologica e la trasformazione digitale Vittorio Colao, nell'ambito della strategia nazionale. A livello di sicurezza, per i dati più sensibili, la soluzione può essere, spiega il Country manager Alessandro Ippolito,



↑ **Alessandro Ippolito**,  
country manager Italia di Oracle

politico, «il cloud pubblico gestito da Oracle a casa del cliente, è il modo migliore per essere compliant, conformi, con tutte le istanze in gioco

ed essere ancora più aderenti alle richieste della strategia nazionale. È, cioè, il punto di partenza per risolvere il problema del Cloud Act», la legge americana che consente agli Usa di richiedere, in alcuni casi eccezionali, i dati conservati nei server dei provider statunitensi anche fuori dal territorio americano.

**Il business del cloud diventa sempre più importante, anche in vista del Pnrr. Che parte del vostro fatturato**

>> continua a pag. 2

### ROBOTIT

## «Dalla chirurgia alla guida autonoma, in rampa di lancio 8 progetti»



↑ **Matteo Elli e Jari Ognibeni**,  
Fondatori di Pariter

**D**alla riabilitazione alla chirurgia robotica. Dalla guida autonoma ai device sui nervi per far muovere gli arti delle persone che non possono deambulare. È l'orizzonte dei progetti di RobotIT, il primo polo nazionale per il Trasferimento tecnologico dedicato alla robotica finanziato da Cdp

>> continua a pag. 4

## «Nelle prossime settimane audiremo il direttore Baldoni»

metro di sicurezza nazionale. Il ministro dell'Innovazione tecnologica, Vittorio Colao, qualche settimana fa evidenziava come il 95% della Pa non fosse ancora in condizione di proteggere i propri dati, come è emerso in modo eclatante nel caso dell'hackeraggio che ha colpito la Regione Lazio, così come ospedali e aziende strategiche. E i dati sull'aumento esponenziale dei crimini informatici purtroppo lo dimostrano. Dobbiamo fare in fretta e fare bene, consapevoli dei rischi e delle potenzialità. Questo è il campo in cui si ridisegnano i nuovi assetti globali, la competitività dell'intero sistema Paese, non solo la protezione dei nostri dati che ne è il presupposto. Il cloud nazionale, la rete a banda larga e le interconnessioni attraverso i cavi marittimi nel Mediterraneo, ma anche lo sviluppo tecnologico e produttivo sui chip e sui semiconduttori, sulle batterie elettriche e ovviamente sulla intelligenza artificiale sono elementi importanti di quella che deve essere una chiara e definita strategia nazionale, condivisa con i nostri partner europei e atlantici.

**Nei piani del Governo c'è il lancio del cloud nazionale della Pa che conterrà anche vari dati sensibili. Sono**

**previsti sistemi di crittografia che dovrebbero proteggere i dati, a seconda anche della loro tipologia. È un sistema sicuro? Avete in programma altre audizioni su questi temi?**

Nelle prossime settimane audiremo il direttore della nuova agenzia per valutare lo stato di attuazione. Intanto auguro buon lavoro al professor Roberto Baldoni e alla sua vice Nunzia Ciardi, eccellenti professionalità. Sono importanti anche le modalità e la tempistica con cui verrà realizzato il Cloud nazionale, per avere assoluta garanzia sulla protezione dei nostri dati. Così come va definita la strategia sulla rete a banda larga.

**Nella partita del cloud entreranno probabilmente anche le big tech in partnership con grandi gruppi nazionali che sono in procinto di fare offerte per il cloud nazionale. Qualcuno paventa però l'applicazione del Cloud Act che consente ai giudici Usa, in determinate situazioni, di richiedere dati anche se conservati in server fuori dagli States. È un pericolo per la sovranità italiana? Come si può risolvere?**

È l'argomento che anche il Copasir ha posto all'attenzione del Governo e credo sia ben presente in chi sta operan-



do per la definizione degli attori e delle regole cui dovranno attenersi, anche in merito alla proprietà della tecnologia e dei dati.

**Sarebbe opportuno arrivare a un protocollo comune in Europa per tutelare la sovranità digitale europea?**

Non è solo una questione di regole ma anche, soprattutto in questo campo, di tecnologia e quindi di sistemi produttivi. Abbiamo molto da fare insieme e certamente il Pnrr può aiutarci a sviluppare meglio le potenzialità europee per garantire una più efficace autonomia e quindi sovranità. Oggi dipendiamo da altri.

**Il suo predecessore, Raffaele Volpi, lamentava un'applicazione blanda del golden power, a tutela degli asset strategici. È un problema persistente? Occorrerebbe un maggiore tute-**

**la per asset come le reti di telecomunicazioni?**

La recente relazione al Parlamento sull'applicazione della golden power nel 2020 fornisce dati inequivocabili: il Governo ha esercitato i poteri di veto solo in 2 casi su 342 notifiche; in altri 42 ha posto condizioni di cui 24 hanno riguardato operazioni societarie e 18 i contesti di fornitura relativi alla tecnologia 5G. Noto però un cambio di passo nel corso di quest'anno, mi sembra che ci sia più consapevolezza nella tutela degli asset strategici, non solo nel campo delle telecomunicazioni; in più contesti la possibilità di esercitare la golden power è stata evocata per scongiurare operazioni ostili con una efficace opera di preventiva moral suasion. Seguiamo con attenzione ■

## >>> DALLA PRIMA PAGINA - PARLA IL COUNTRY MANAGER ITALIA DI ORACLE

**rappresenta il cloud in Italia e quali sono i vostri piani?**

Siamo di fronte a un processo di forte adozione del cloud sia da parte delle imprese sia da parte della Pa. Ora, con il Pnrr, c'è un impulso forte, impresso dal Governo, sui processi di digitalizzazione. Per noi, al momento, il cloud rappresenta circa il 25-30% dei nostri ricavi a livello globale, con punte più alte in alcuni Paesi a seconda dei trimestri, ma in Italia prevediamo una crescita. In più, a breve, è nei nostri progetti l'apertura della nuova "cloud region" italiana, a Milano. In generale, dal punto di vista dei conti, il business italiano va molto bene, da molti trimestri, e su molte direttrici, non solo quella del cloud.

**Quando è previsto il taglio del nastro per il data center di Milano?**

Contiamo di aprire entro la fine dell'anno.

**Come potete contribuire al progetto di cloud nazionale?**

Le direzioni chiare del Pnrr, della strategia di cloud nazionale e di quella dei dati messe in campo dal Governo ci stanno coinvolgendo molto. In particolare, io sono un sostenitore del progetto di cloud

nazionale. Oracle, dal canto suo, può offrire la maturità dei suoi servizi cloud, la capacità d'innovazione e investimento e lo sviluppo della tecnologia su cui è da sempre un'esperta, il data management. Inoltre, noi possiamo offrire una soluzione unica, che già vendiamo, e cioè il "cloud pubblico portato a casa del cliente" ("cloud at customer"), che garantisce la sicurezza e la gestione del dato nel data center del cliente, quindi in settori regolamentati dove è richiesta la residenza o sovranità dei dati entro i propri confini, tipicamente nella Pa e nel settore bancario e finanziario. Puntiamo inoltre a raggiungere l'obiettivo di mettere a fattor comune i dati tra le Pubbliche amministrazioni e tra le Pubbliche amministrazioni e i cittadini. Poi speriamo di dare il nostro contributo anche con il nostro cloud data center che sarà aperto a Milano. Sempre nel capoluogo lombardo stiamo inoltre per aprire la nostra nuova sede, in zona più centrale, che dovrebbe essere operativa nei primi mesi del 2022. Siamo presenti anche a Roma, con una sede estremamente importante vista la centralità che per noi, storicamente, rappresenta il mercato della Pa.

**Parteciperete alla selezione in corso per il cloud nazionale?**

Siamo ben posizionati a tutti i livelli e con tutte le aziende per essere parte di questo progetto.

**Come ovviare ai problemi del Cloud Act, la legge che consente ai giudici Usa di richiedere in determinate circostanze i dati conservati dalle multinazionali statunitensi anche fuori dal territorio americano?**

Quello del Cloud Act è un tema importante. Secondo noi la soluzione del "cloud at customer" cioè il cloud pubblico gestito da Oracle a casa del cliente, è il modo migliore per essere compliant, conformi, con tutte le istanze in gioco ed essere ancora più aderenti alle richieste della strategia nazionale. È, cioè, il punto di partenza per risolvere il problema del Cloud Act. Per quanto riguarda soprattutto i dati critici, sensibili, stiamo già fornendo la nostra tecnologia in maniera trasparente a vari clienti. Tra quanti si avvalgono delle nostre soluzioni applicative in cloud (SaaS), ci sono: Poste Italiane, Mondadori. Tra i clienti che si avvalgono della nostra soluzione "cloud at customer" si contano Inail, Deutsche Bank, Credit Agricole e altre realtà della Pa e del mondo bancario. ■

# «Occorrono tutele tecniche e garanzie nei contratti per risolvere il nodo del Cloud Act»

L'applicazione o meno del Cloud Act americano alle aziende che si occuperanno della cosiddetta "Nuvola di Stato" è uno dei nodi da risolvere in vista dell'avvio della strategia nazionale sul cloud. L'obiettivo è impedire cioè che giganti come Google o Microsoft siano costretti dalla legge americana del 2018 ad alzare il velo, in alcuni casi eccezionali, sui dati conservati nei propri server. Contrariamente a chi ritiene che sia fondamentale un accordo diplomatico tra Italia e Usa (vedi il giurista Innocenzo Genna su Digit Economy del 9 settembre), Massimiliano Masnada, partner responsabile del team di Privacy e Cybersecurity di Hogan Lovells in Italia, che assiste importanti cloud computing provider americani e internazionali, spiega che bastano tutele tecniche e garanzie nei contratti. «Ci sono innanzitutto - spiega Masnada a DigitEconomy24 (report del Sole 24 Ore e della Luiss Business School) - due ordini di problemi principali: bisogna garantire la sicurezza del cloud italiano e c'è l'esigenza di mettere al riparo i dati dei cittadini rispetto a una possibile ulteriore attività di trasmissione non autorizzata a soggetti terzi. Bisogna a questo punto chiedersi: è in grado il cloud italiano di garantire gli stessi elevati standard di sicurezza dei grandi provider internazionali?»

I dati sugli attacchi informatici, prosegue il legale, sono su questo fronte emblematici e mostrano l'importanza di difendere la sicurezza degli italiani. «Nel 2020, a livello mondiale, secondo Clusit, (l'associazione italiana per la sicurezza informatica) l'incremento degli attacchi cyber a livello globale è stato pari al 12% rispetto all'anno precedente. Di recente c'è poi stato il caso emblematico della Regione Lazio dove, per aver lasciato un programma aperto, sono stati rubati i dati dei cittadini». Dal punto di vista della sicurezza, insomma, «chi garantisce maggiormente la tutela sono coloro che hanno acquisito un'enorme esperienza in questa attività. In pratica, non si può cercare l'eccellenza nel solo ambito territoriale italiano se questa eccellenza non è facilmente rintracciabile».

La soluzione? «Dare l'intera gestione del cloud a una multinazionale americana può creare problemi sia giuridici sia politici. In tal senso l'intervento del ministro Colao al meeting di Cernobio è stato chiarissimo. Occorre, invece, riservare la gestione a un grande soggetto nazionale, accompagnandola però con accordi di fornitura o di partnership con i grandi provider che possano mettere a disposizione del provider italiano la loro grande esperienza e capacità. Per evitare la sca-

labilità a livello internazionale dei dati italiani possono essere predisposte tutele adeguate sia dal punto di vista tecnico, come le chiavi crittografiche, sia dal punto di vista contrattuale, ottenendo cioè la garanzia che i dati non vengano ulteriormente ceduti».

In sostanza le leggi che ci sono, come ad esempio, «le previsioni del regolamento Ue numero 679 del 2016 in tema di trasferimento di dati extra-Ue e di per sé sufficienti, ma a livello regolamentare si possono creare ulteriori framework che impediscano l'accessibilità da parte di terzi». Il Cloud Act, chiarisce il legale, «si applica ai provider americani e, in generale, ad operatori sottoposti alla giurisdizione degli Stati Uniti che conservano all'interno del cloud di loro proprietà i dati da chiunque essi provengano. Nel momento in cui si creano cloud e warehouse data che fuoriescono dalla giurisdizione degli Usa si è già tutelati dall'applicazione del Cloud Act. Facciamo un esempio: se io compro una macchina italiana che ha componenti forniti da un gruppo straniero, la gestione dei componenti che fanno parte della macchina e dei dati è, in generale, appannaggio solo del produttore e non anche del fornitore. La gestione del cloud nel suo complesso nonché delle chiavi crittografiche possono, cioè, essere gestite dall'Italia anche



↑ **Massimiliano Masnada**, partner responsabile del team di Privacy e Cybersecurity di Hogan Lovells in Italia

se fornite da un provider straniero. Ciò non significa che il provider abbia libero accesso ai dati».

Tirando le somme, «da un punto di vista logico, e nell'interesse dei cittadini italiani, credo non si possano avere preclusioni all'uso di applicativi forniti da un terzo solo perché è americano. Quello che interessa di più ai cittadini è garantire che il cloud sia sicuro, in grado di mettere la Pa nelle condizioni di fornire in tempi rapidi i propri servizi. La materia è in divenire, ma interessa tutti, visto che il Pnrr prevede circa 900 milioni di euro per il cloud nazionale». In questo panorama, il Garante della privacy «sarà sicuramente - conclude Masnada - un interlocutore necessario e auspico che vi sia un atteggiamento non ideologico ma concreto, sulla base di quanto finora fatto rispetto alla gestione dei dati». ■

## Attacchi ransomware in Italia saliti del 144% in sei mesi

La pandemia ci ha posto di fronte a una serie di nuove sfide, nonché di nuove minacce informatiche. Secondo i dati di Check Point Research, gli attacchi ransomware, cioè gli attacchi che rendono inaccessibili i dati dei computer infettati, chiedendo poi un riscatto, sono cresciuti negli ultimi sei mesi e le organizzazioni colpite sono aumentate del 144 per cento. Mentre a livello globale il numero medio di attacchi ransomware è aumentato del 20% di settimana in settimana nei mesi di aprile e maggio, del 41% nella prima metà dell'anno, e del 93% negli ultimi 12 mesi. Dato il livello di rischio estremamente elevato che questo rappresenta

per le aziende e per la sicurezza dei loro dati, la società Check Point Software sottolinea l'importanza cruciale di riabilitare i dati rubati o criptati di un'azienda nel caso in cui cada vittima di un cyber-criminale. Per questo, gli esperti di sicurezza elencano cinque ragioni per cui le aziende dovrebbero fare del backup la loro priorità: le misure preventive non sempre funzionano, gli attacchi informatici si evolvono; il furto di dati compromette la reputazione aziendale; il cloud diventa un altro vettore di attacco e i pericoli interni sono a volte indecifrabili, ed è quindi essenziale formare i dipendenti sulle diverse tecniche e sul corretto approccio alla

sicurezza informatica. Far capire l'importanza di avere backup aggiornati per qualsiasi imprevista evenienza o per un attacco può essere, dice Check Point Software, una delle migliori difese. ■



# A breve in arrivo nuovi partner per RobotIT

Venture Capital, affiancata dalla holding Pariter (che di volta in volta potrà anche fare da co-investitore nei progetti). L'obiettivo è sostenere la nascita di nuove start up ideate all'interno delle Università e nei centri di ricerca. Al momento, secondo quanto riferito a DigitEconomy.it (report del Sole 24 Ore Radiocor e della Luiss Business School) dai fondatori di Pariter, Matteo Elli e Jari Ognibene, sono stati visionati 80 progetti, con 15 in rampa di lancio per poi arrivare a selezionarne otto l'anno, e un impatto di investimento fino a due milioni di euro.

Nuove realtà, inoltre, si affacceranno a breve, raccontano Elli e Ognibene: «saranno partner per la gestione della proprietà intellettuale, del supporto per le tematiche elettroniche. Stiamo creando un ecosistema completo per mettere basi solide». Pariter è nata nel 2017 con l'obiettivo di creare un'entità di investimento in società deep tech basate in Italia, che sviluppano cioè tecnologie abilitatrici di innovazione spinta. Nel corso degli anni Pariter, che oggi raccoglie oltre 200 investitori, «si è evoluta ed è diventata – raccontano i fondatori – il principale network di investimento dedicato al deep tech. Investiamo sia sul fronte di iniziative pre-company, diventando in pratica il primo investitore, sia nella fase tradizionale di start up».

Ora, con RobotIT che conta tra i primi partner Leonardo, si apre un nuovo orizzonte. «Si tratta – spiega Elli – di un veicolo di investimento, un polo, un ecosistema che mette assieme le quattro componenti principali: capitale, istituzione, corporate e ricerca». Pariter, dal canto suo, «gestirà le iniziative in termini di scouting, identificazione dei team, validazione della tecnologia, selezione delle opportunità di investimento. Abbiamo la possibilità di entrare nei centri



↑ Chirurgia operatoria a distanza

di ricerca, valutare la tecnologia. A qualche mese dall'inizio dell'attività di RobotIT, ora c'è un panorama più preciso sui progetti che saranno privilegiati: «si tratta di tematiche molto interessanti, legate al mondo della riabilitazione robotica, della chirurgia robotica, ai servizi legati al mondo di ristorazione, alla riabilitazione degli arti inferiori, sistemi per automazione e abilitazione di tutto il mondo dell'auto autonoma, dei veicoli a guida autonoma. C'è un team, ad esempio, che ha sperimentato con buoni risultati l'inserimento di alcuni device sui nervi; abilitando il controllo dell'esterno riesce, cioè, ad azionare il movimento del corpo in soggetti che non possono farlo in autonomia. Sono più avanti i temi della abilitazione robotica sugli arti o anche l'applicazione della robotica in ambito automotive e ferroviario per la guida autonoma. Un po' più indietro, ad esempio, è il tema della chirurgia robotica». Per vedere queste applicazioni sul mercato ci vorrà comunque molto tempo,

considerando la fase della certificazione, dell'approvazione, dell'affinamento della tecnologia per un ciclo di vita completo che dura dai due ai quattro anni. Tuttavia, spiegano Elli e Ognibene, «può succedere che dopo poco una società sia interessata, anche se non è certificata e non è ancora pronta. In questo caso i tempi si accorciano».

RobotIT è il primo progetto che apre una serie di investimenti del genere. Cdp Venture Capital, infatti, attraverso il fondo di technology transfer, con una dotazione di 275 milioni di euro, investirà in tutta la filiera del trasferimento tecnologico attraverso la creazione di poli nazionali distribuiti sul territorio. RobotIT è il primo. L'investimento iniziale, già stanziato da parte di Cdp Venture Capital e dagli altri fondi specializzati, è di 40 milioni, con un effetto leva stimato complessivo di oltre 100 milioni di euro in 4 anni per la creazione e lo sviluppo di più di 50 nuove aziende. ■

## Nonostante i timori di cybersecurity cresce la richiesta di cloud

I timori per la cybersecurity sono una realtà, ma le aziende vogliono ugualmente il cloud. È quanto emerge dai dati dell'Equinix 2020-31 global tech trend survey, uno studio annuale condotto su 2.600 responsabili It nelle Americhe, Asia-Pacifico ed Emea. La necessità di rimanere competitivi e soddisfare le richieste degli utenti ha portato a un aumento, rispetto all'anno precedente, dal 15% al 37%, delle aziende che affermano di voler trasferire, nonostante le crescenti preoccupazioni legate alla cybersecurity, le applicazioni business-critical nel cloud. Oggi si stima che quasi la metà (47%) dell'infrastruttura It a livello globale sia sul

cloud, non a caso 7 leader It su 10 ritengono che la migrazione verso il cloud rappresenti una priorità per l'infrastruttura digitale del futuro. Dallo scoppio della pandemia globale da Covid-19, però, il rischio di cyberattacchi si è notevolmente ampliato. In Italia, più di due terzi (71%) dei responsabili It prevede di spostare più funzioni sul cloud (dato leggermente in calo rispetto al 79% dell'anno scorso) e l'89% degli intervistati ritiene che migliorare la cybersecurity dell'azienda sia un'altra priorità assoluta nel nostro Paese. Lo scopo dello studio presentato, afferma Emmanuel Becker, managing director di Equinix Italia, «è indagare sulle

necessità e le preoccupazioni delle aziende così da supportarle e aiutarle ad accelerare la loro trasformazione digitale. La migrazione di funzioni verso il cloud è una componente chiave di una solida infrastruttura digitale, ma molti leader digitali sono

cepiti. In Equinix, stiamo lavorando con i leader digitali per mitigare i rischi, offrendo una piattaforma interconnessa che consente lo scambio diretto e sicuro di dati tra le aziende per sostenere il successo futuro dei clienti».



← Emmanuel Becker, managing director di Equinix Italia