18-MAR-2024
da pag. 1-2 / foglio 1 / 2

L'Economia del CORRIERE DELLA SERA
Settimanale - Dir. Resp.: Luciano Fontana
Tiratura: N.D. Diffusione: N.D. Lettori: 1728000 (DS0001948)

DATA STAMPA
www.datastampa.it

LE LEGGI CI SONO E SONO BUONE
IL RISCHIO È LA FRAMMENTAZIONE

ATTACCHI E DIFESA HI-TECH CI PENSI LO STATO (NON LE REGIONI)

di **FERRUCCIO DE BORTOLI**

Quando Mario Monti, presidente del Consiglio — ormai un'era geologica fa — si sentì chiedere all'improvviso da Barak Obama che cosa stessimo facendo sulla *cybersecurity*, fu istintivo per lui voltarsi verso i suoi accompagnatori. Con un'aria sinceramente interrogativa. Di che cosa esattamente stava parlando il presidente degli Stati Uniti?

Cominciò allora un cammino virtuoso. Tutto grazie a un provvedimento del 2013, la prima disciplina della materia. Si coinvolsero 45 atenei, circa 200 docenti universitari, la struttura dei Servizi, istituzioni scientifiche e culturali e ovviamente le aziende più tecnologicamente avanzate. Con il governo Gentiloni, nel 2017, si creò una struttura ad hoc, all'interno del Dis, il Dipartimento informazioni per la sicurezza. Nel 2021, con l'esecutivo Draghi, dopo il clamoroso attacco *hacker* ai dati sanitari della Regione Lazio, venne costituita l'Agenzia nazionale per la cybersecurity (Acn) oggi presieduta dal prefetto Bruno Frattasi. Il suo predecessore, Roberto Baldoni, esce in questi giorni con un saggio (*Charting digital sovereignty, a survival playbook*) sul tema del controllo statale del cyberspazio, sulla sicurezza nazionale dei dati e, in generale, sulla sovranità digitale.

LO SCUDO DIGITALE

DATI & PIRATI INVESTIAMO DI PIÙ SULLA PROTEZIONE

Con una premessa importante. Qui non si tratta semplicemente di difendersi da incursioni di *phishing* e *malware* e da altre minacce informatiche, peraltro moltiplicatesi nel 2023 anche se non nella misura che viene accredita sul prospero mercato degli antivirus. Vi sono stati in totale 1411 eventi cibernetici, cresciuti del 30% rispetto al 2022, di cui 168 attacchi *ransomware*, ovvero siti infettati con richiesta di riscatto (il 625% in più). Gli attacchi Ddos (Distributed denial of service), inondazioni che bloccano il servizio, sono aumentati del 27%. In cima ai dati sensibili da proteggere ce n'è uno decisamente superiore: la qualità e la libertà del nostro sistema democratico. Dunque, prima di tutto, selezioniamo le persone che devono occuparsene sulla base delle competenze e non delle appartenenze come purtroppo è in parte accaduto con il governo Meloni.

Nonostante tutte le difficoltà e i ripetuti cambiamenti di governo, abbiamo recuperato in questi anni diverse posizioni. Siamo tra i dieci Paesi meglio organizzati nel prevenire e respingere gli attacchi cibernetici. Al punto che l'ultimo Cybersecurity Act statunitense riprende addirittura alcune disposizioni contenute nei decreti italiani, approvati tra il 2019

ARTICOLO NON CEDIBILE AD ALTRI AD USO ESCLUSIVO DEL CLIENTE CHE LO RICEVE - DS1948 - S.11677 - L.1956 - T.1745

L'Economia del Corriere della Sera
Settimanale - Dir. Resp.: Luciano Fontana
Tiratura: N.D. Diffusione: N.D. Lettori: 1728000 (DS0001948)

DATA STAMPA
www.datastampa.it

e 2021, per imporre misure di sicurezza sui software critici, tra cui l'obbligo di notifica delle aziende strategiche attaccate. Una piccola soddisfazione.

Morale: se veramente riteniamo che la sovranità digitale sia una materia decisiva per il nostro benessere futuro e per il livello delle nostre libertà, allora non può essere che bipartisan, frutto di una consapevolezza trasversale e soprattutto popolare. Tocca tutti. La riservatezza dei compiti, legata alla sicurezza nazionale e atlantica non può essere avvolta in una sorta di opacità quasi romanzesca. Il cittadino normale, la piccola e persino media azienda pensano (sbagliando di grosso) che il problema non li riguardi. E che sia una materia così complessa e sofisticata da essere di esclusiva pertinenza degli Stati.

Lo stato delle cose

Il saggio di Baldoni si incarica (purtroppo non nella nostra lingua ma tant'è) di sfatare questo mito un po' letterario. Individua ben nove modalità di attacchi cibernetici ai danni delle industrie nazionali; ipotizza scenari inquietanti sull'uso futuro dei computer quantici; dimostra come una normale applicazione di intelligenza artificiale possa manipolare struttura e andamento di mercati non solo azionari. E lancia un vero grande allarme che riguarda la cosiddetta *workforce*. Rischiamo un drammatico vuoto di talenti.

Poi c'è un dilemma delicato. Ed è nel rapporto tra il pubblico — chiamato ad applicare le regole — e il privato che possiede la tecnologia e ha un potere così vasto che gli consentirebbe in teoria di prescindere totalmente da ogni aspetto normativo, anche se europeo. I grandi provider di *cloud* al mondo sono sette. Sfuggendo giustamente da influenze cinesi e a maggior ragione russe, sarebbe anche il caso di chiedersi, con tutto il rispetto, se consegnare anche dati considerati strategici ai partner americani risponda fino in fondo ai conclamati criteri di sovranità digitale, soprattutto con i sovranisti al governo. Il Polo strategico nazionale (Psn), voluto fortemente da Vittorio Colao quando era ministro alla Transizione digitale, è frutto di una collaborazione tra pubblico e privato. Gli azionisti della società, guidata da Emanuele Iannetti, sono Tim al 45%, Leonardo al 25, Cdp Equity al 20 e Sogei al 10. Psn è fuori dal Cloud Act americano e può usare, per i dati più critici e soprattutto quelli ritenuti strategici, la tecnologia di altri, per esempio Google e Oracle, gestendosela in casa. Ma certamente il *cloud* italiano per essere più forte e sicuro ha bisogno di un processo industriale di accentramento dei servizi e degli operatori nazionali veloce e coerente.

Che cosa è accaduto finora? Da una parte le amministrazioni centrali, con l'eccezione del Ministero dell'Economia e delle Finanze (che però ha Sogei), hanno realizzato comunque una migrazione dei loro servizi e dei loro *data center* verso il Psn. Anche perché, in caso contrario sarebbero stati messi in discussione, i finanziamenti del Piano nazionale di ripresa e resilienza (Pnrr). Le Regioni sono andate invece in ordine sparso, potenziando le loro infrastrutture. Soprattutto quelle che hanno corposi servizi in house. La più resistente è il Friuli-Venezia Giulia. Le adesioni comunque sono state differenziate e questo non impedisce un processo di razionalizzazione, seppur allungato da proroghe necessarie (l'ultima concessa dall'Acn è comunque scaduta il 31 gennaio scorso). Certo lo complica soprattutto di fronte a salti tecnologici (dall'intelligenza artificiale all'Internet of things) che le Regioni da sole, per quanto attrezzate (in particolare l'Emilia Romagna), non potranno seguire.

Inoltre si sta preparando una certificazione europea. Il 31 gennaio la Commissione di Bruxelles ha adottato un regolamento, elaborato dall'Agenzia europea per la cybersecurity (Enisa), che ha lo scopo di rafforzare la sicurezza di prodotti, servizi e processi nel mercato unico. Il primo passo riguarda proprio il cloud europeo che è il fronte più delicato. Siamo sicuri che tutte le Regioni, oltre al Psn, potranno essere certificate? La sovranità digitale non è purtroppo la sommatoria di tante piccole e orgogliose sovranità regionali.

© RIPRODUZIONE RISERVATA

Siamo tra i 10 Paesi più organizzati nel prevenire e respingere gli attacchi cibernetici. Ora gli americani hanno «copiato» da noi l'obbligo di notifica da parte delle aziende sotto scacco

Ma al «cloud» tricolore, frutto di una collaborazione tra pubblico e privato e fuori dall'orbita dei big Usa, per essere più forte serve un accentramento di servizi e operatori. Al momento, invece, c'è stata la migrazione di molte amministrazioni centrali mentre le Regioni sono andate in ordine sparso. E intanto si parla di certificazione Ue...

ARTICOLO NON CEDIBILE AD ALTRI AD USO ESCLUSIVO DEL CLIENTE CHE LO RICEVE - DS1948 - S.11677 - L.1956 - T.1745