NOVA24 – 11 GENNAIO 2015

Chi difende il nascente Stato digitale italiano?

di Biagio Simonetta

Correre veloci verso l'e-government è la parola d'ordine degli ultimi mesi. La digitalizzazione delle pubbliche amministrazioni è una priorità, e appartiene a quell'insieme di cose dalle quali non si può prescindere se si vuol fare ripartire il Paese. Del resto, non solo il futuro ma già il presente è nei dati. Occorre sbrigarsi, dunque.

Dal marzo 2012 all'ottobre scorso, l'Italia è cresciuta molto in fatto di open data, e sono stati resi disponibili oltre 12mila dataset. Anche se a sbirciare la cartina geografica fornita dal Governo traspare in modo netto la discrepanza enorme fra Nord e Sud del Paese (si digitalizza quasi esclusivamente dalla Toscana in su, nda). Segno che la Questione Meridionale è tematica quanto mai attuale, anche nell'epoca dei big data. Il ritmo della digitalizzazione è comunque buono, e lascia ben sperare. Tanto che pensare di ottenere un certificato di residenza con pochi click sul proprio smartphone non è più fantascienza, ma appartiene a un genere di azioni abbastanza prossime.

Se da un lato, però, la corsa all'e-government procede spedita e quasi entusiasma, dall'altro c'è l'ombra buia della sicurezza informatica ad aleggiare pesantemente sugli scenari futuri. Quando tutto sarà digitale (cioè molto presto), quanto saranno esposte le nostre identità? Con l'anagrafe, le cartelle sanitarie, l'andamento scolastico e accademico di ogni cittadino tramutati in dati e conservati su una "nuvola", quanto saremo al sicuro?

Inutile dire che in questo contesto lo spettro del furto di identità diventa enorme. Un po' perché la digitalizzazione delle Pa sposa benissimo la golosità degli hacker, alla continua ricerca di identità da clonare. Un po' perché lo stato della sicurezza informatica, in Italia, è da sempre una nota dolente.

Andrea Rigoni, esperto di cyber security e consigliere del Governo Letta per l'Agenda digitale, non nasconde le sue preoccupazioni: «Non conosciamo lo stato della sicurezza nella Pa. Possiamo presumere che, poiché non vi sono controlli di sicurezza, il livello complessivo sia molto basso. Non esistono standard a cui le amministrazioni si devono attenere, né veri e propri controlli». Rigoni racconta anche dell'incapacità attuale di rilevare eventuali attacchi: «Non abbiamo una capacità di rilevazione e risposta agli incidenti, pertanto è possibile che la maggior parte degli attacchi passino inosservati. Considerata la situazione degli attacchi resi noti negli ultimi anni, mi viene difficile pensare che la nostra Pa sia esente da questi fenomeni. È più facile presumere che nessuno se ne accorga».

Anche Aldo del Bò, italianissimo marketing director di Kaspersky, ci va giù duro e parla di «obsolescenza delle infrastrutture italiane, incapaci quindi di essere protette rispetto alle minacce». Del Bò, durante l'evento di Kaspersky a Barcellona, si è detto convinto che nel processo di digitalizzazione della Pa si debba tener conto della «vulnerabilità della tecnologia nostrana, che predilige l'argomento della sicurezza fisica del lavoro, senza considerare la sempre più necessaria combinazione di questa con quella logica, cioè con quella delle macchine e del software che pilota le macchine». E quando a del Bò chiediamo perché, nonostante la scarsa sicurezza, attualmente non arrivano grosse notizie di attacchi informatici, la risposta è sibillina: «Diciamo che di attacchi ne subiamo, eccome. I nostri laboratori misurano oltre 300mila campioni infetti su base quotidiana. Ma diciamo anche che per varie ragioni non si comunica abbastanza, o abbastanza bene».

Da Helsinki, dove adesso le notti sono infinite e i giorni durano niente, il milanese Paolo Palumbo (oggi senior researcher di F-Secure) non ha dubbi: «La sicurezza informatica è un aspetto che deve essere parte integrante della pianificazione, dello sviluppo e dell'operatività dei sistemi che gestiscono informazioni digitali, non un qualcosa di cui ci si ricorda solo a cose fatte». Proprio questo è il rischio più concreto dell'Italia digitale. Le possibilità di trovarci in un Paese digitalizzato ma estremamente vulnerabile sono altissime. E gli hacker sono in agguato.