Oggi la «fuga di notizie» corre sulla rete…

WikiLeaks stravolge il giornalismo tradizionale ed inaugura l'era dei leaks, la fuga di notizie rilasciate online. Di questo scrive Philip Di Salvo nel suo libro «Leaks. Whistleblowing e hacking nell'età senza segreti», presentato in occasione della Biennale Tecnologia. Ma il whistleblowing nasce grazie alla rivoluzione digitale? Ovviamente no. Molte notizie in passato sono state rivelate grazie ad informatori anonimi, si pensi al caso Watergate. La vera rivoluzione sta nella rapidità di comunicazione delle informazioni, che grazie alla piattaforma di WikiLeaks possono essere inoltrate alla redazione dalla propria abitazione, e nella protezione delle fonti, che restano anonime grazie ai sistemi di crittografia. L'altra faccia del whistleblowing digitale è, di fatto, l'hacking della sfera politica, attività illegale che mette a rischio gli attivisti, come nei casi Manning e Snowden, ecco perché sorge la necessità di sfruttare l'ecosistema digitale per aumentare la sicurezza dei whistleblower. Le nuove tecnologie, che permettono di accedere ai contenuti in modo rivoluzionario rispetto al passato, spesso danno la possibilità alle testate giornalistiche di accedere ad informazioni di natura controversa che non coinvolgono solo i soggetti pubblici ma l'intera comunità mondiale, oggi sottoposta a sistemi di controllo diffuso proprio grazie alla digitalizzazione. Per questo si evidenzia l'eticità dell'attività di hacking, diversa dal cosiddetto cracking, che porta con se una serie di valori, tra cui la responsabilità civica di comunicare alla società «che cosa c'è dentro alla scatola». L'altra novità derivante dalla democraticizzazione fornita dalle tecnologie digitali ed è il network journalism: la documentazione degli eventi tramite post sui social media, che trasforma il ruolo dei giornalisti da cassa di risonanza a filtro delle notizie. Il sistema di informazione moderno – conclude Di Salvo - è estremamente complesso e a volte rischioso, è indispensabile quindi che il giornalismo riconosca il proprio ruolo e si immetta nel sistema con il giusto rapporto di forza tra testate tradizionali e social network.

Jasmine MILONE

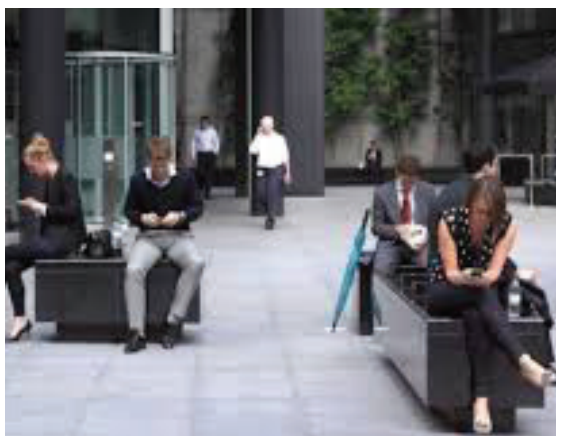
APOSTOLATO DIGITALE

condividere codici di salvezza

DIGITAL DIVIDE GEOGRAFICO – COSA SONO AREE GRIGIE E BIANCHE

Sui piccoli comuni, l'«ostacolo» del divario digitale

Come nel mondo reale anche nel mondo virtuale quel che conta è «unire» e non «dividere».
La rete è diventata una estensione della nostra cultura, delle nostre storie e della nostra memoria, e alla rete spesso ci affidiamo per comunicare o per sentirci un po' meno soli.
La rete può quindi metterci più facilmente in relazione attivando nuove dinamiche sociali e, pur senza sostituirsi alla rete dei contatti fisici, può contribuire ad unirci.
Non c'è peraltro progresso senza le infrastrutture e la rete e, quindi, tutti noi dovremmo avere una connettività veloce, utile per garantire l'equità sociale nell'accesso ai servizi digitali in ogni area del territorio nazionale.
Il «digital divide» o «divario digitale» è una nuova forma di divario sociale da colmare e riguarda coloro che hanno un accesso effettivo alle tecnologie dell'informazione e coloro che ne sono esclusi. È un divario che può dipendere dalle condizioni economiche, dal livello di istruzione, dalle differenze di età, di sesso, di etnie o anche da fattori geografici.
Il «digital divide» geografico riguarda le aree metropolitane che hanno accesso alle tecnologie dell'informazione e le altre aree che ancora ne sono escluse o ne hanno un accesso limitato. Tra le aree maggiormente penalizzate ci sono proprio i piccoli comuni, spesso ubicati in località lontane dalle aree metropolitane e in luoghi non facilmente accessibili. Risale al lontano 2015 il documento con cui viene descritta la strategia italiana per la banda ultra-larga con la suddivisione del territorio nazionale in sotto-aree: bianche, grigie e nere. La distinzione in aree fu effettuata ai fini della valutazione e della successiva assegnazione degli aiuti di stato.
Le aree bianche sono quelle prive di reti ultra-broadband, le aree grigie sono le aree in cui è presente o verrà sviluppata una rete da almeno un operatore privato, le aree nere sono quelle in cui verranno sviluppate almeno due reti ultra-broadband di operatori diversi.
Sono ancora tante le aree bianche e in queste vi sono soprattutto i piccoli comuni, distanti dalle aree metropolitane e sovente situati in aree di difficile accesso. Le aree bianche sono oggetto di interventi dello stato e di privati volti ad accelerare i tempi per assicurare la disponibilità della banda larga che si basa sulla tecnologia ad onde radio. Gli operatori del settore si stanno orientando verso la Fwa per ridurre il gap esistente tra le zone ben cablate e le restanti zone. Il wireless Fwa è una valida alternativa alla fibra soprattutto nei piccoli comuni dove è più complicato portare quest'ultima e si basa sulla presenza capillare delle antenne della vecchia Tv analogica.
Lo sviluppo economico e sociale delle aree dei piccoli comuni dipenderà pertanto dalla capacità di programmare e vincere in tempi rapidi la sfida della digitalizzazione con il completamento del potenziamento delle reti nelle aree bianche. Le reti e la digitalizzazione sono indispensabili premesse per portare sviluppo e benessere economico in tali aree, per il ripopolamento dei piccoli comuni e per un nuovo equilibrio tra aree metropolitane e il resto del territorio. L'innalzamento tecnologico e il miglioramento della rete dei trasporti nei piccoli comuni, potrà consentire la creazione di nuove start-up, di FabLab e di nuovi posti di lavoro, ma anche di effettuare lo smartworking nei luoghi di origine senza dover affrontare faticosi spostamenti verso le aree metropolitane. È possibile dunque creare una inversione di tendenza, ripopolare le aree dei piccoli comuni e migliorare la qualità di vita di tante persone che non dovranno abbandonare i propri luoghi di origine perché avranno la possibilità di scegliere di lavorare e di viverci.



Le reti e la digitalizzazione sono indispensabili premesse per portare benessere

Vito COVIELLO
Responsabile AIDR Osservatorio tecnologie digitali settore trasporti

Perimetro nazionale di sicurezza cibernetica, al via il progetto

Un Perimetro Nazionale di Sicurezza Cibernetica per le funzioni vitali dell'Italia: è entrato in vigore il 5 novembre il primo Decreto per l'attuazione del progetto.
Sarà uno scudo difensivo per proteggere le Pubbliche Amministrazioni e le aziende fondamentali da attacchi informatici: inizia a prendere forma in questi mesi con il censimento dei soggetti che entreranno nel sistema di protezione. «Questo decreto è il primo dei passi attuativi del Perimetro, e in sé non costituisce nulla di inatteso» afferma Corrado Giustozzi, esperto di cybersecurity presso l'Agenzia per l'Italia Digitale: «era infatti previsto dalla norma principale, che ha delegato la regolazione degli aspetti operativi dell'attuazione del Perimetro ad una serie di Dpcm».
Concretamente il primo passo che si sta muovendo consiste nel censire i soggetti che effettuano funzioni essenziali per lo Stato e vanno perciò protetti. Si tratta di enti "che assicurino la continuità dell'azione di Governo e degli Organi costituzionali, la sicurezza interna ed esterna e la difesa dello Stato, le relazioni internazionali, la sicurezza e l'ordine pubblico, l'amministrazione della giustizia, la funzionalità dei sistemi economico e finanziario e dei trasporti» recita il testo del Dpcm 131/2020. In tutto saranno riuniti in 150 tra pubblici e privati in una lista segreta e saranno in stretto rapporto con le Agenzie per la Protezione Digitale: se saranno vittime di cyber attacchi dovranno avvisare entro 6 ore lo Csirt (Computer Security Incident Response Team – Italia), gruppo di esperti presso la Presidenza del Consiglio dei Ministri. In caso di grave violazione, verrà inoltre attivato l'Nsc, il Nucleo per la Sicurezza Cibernetica presieduto dal professor Roberto Baldoni il cui compito è quello di proporre al Presidente del Consiglio una possibile risposta all'attacco e coordinare il ripristino del servizio.
Una volta individuati gli enti da proteggere, il secondo passo sarà il censimento dei beni informatici di pertinenza di ciascuno, mentre verrà istituito un tavolo interministeriale per l'attuazione del Perimetro di Sicurezza Nazionale. Le previsioni iniziali avrebbero voluto il sistema a regime per la primavera 2021, ma a causa della pandemia i tempi saranno necessariamente rallentati: il prossimo Dpcm con ulteriori sviluppi del progetto è atteso entro sei mesi.

Simone GARBERO

Fondazione Leonardo
Civiltà delle Macchine: per coniugare conoscenza scientifica e umanesimo digitale.