Rassegna del 23/03/2018

IMMIGRAZIONE

ECONOMIA E FINANZA

TRASPORTI, POSTE E TELECOMUNICAZIONI

Avvenire
23-MAR-2018
pagina 25
foglio 1

Etnocom, comunicazione per migranti

La prima agenzia pensata per i 6,5 milioni di stranieri presenti in Italia

PAOLA SCARSI
ROMA

Nel 2006, un gruppo di professionisti della comunicazione si è fermato a osservare gli immigrati. Chi sono? Dove vivono? Che progetti hanno? Che prodotti consumano? Così è nata l'idea di Etnocom, con sede a Roma, prima e unica agenzia italiana di comunicazione etnica.
«L'impulso – spiega l'amministratore delegato Filippo Ielmini – arrivò quando Poste Italiane e Money Gram siglarono l'accordo per il trasferimento di denaro all'estero e dovettero comunicarlo ai quasi due milioni di stranieri presenti in Italia: realizzammo una comunicazione mirata per ciascuna nazionalità, etnia e lingua». Oggi in Italia ci sono sei milioni e mezzo di stranieri: rappresentano un fenomeno sociale e una grande opportunità commerciale. «Ci rivolgiamo a loro conoscendone e rispettandone cultura, tradizioni, abitudini e comportamenti, studiandone stili di vita e di consumo per offrire ad aziende e istituzioni italiane un nuovo target ed aiutandole a comunicare con loro. Rivolgersi a persone così differenti da noi e tra di loro non significa tradurre, ma conoscere; effettuiamo ricerche con la Doxa ed abbiamo ideato modelli di marketing e commerciali». Un'intuizione che ha avuto grande successo: «Cresce il numero e la tipologia di aziende che investe su questi nuovi consumatori; realizziamo campagne in 15 lingue, con il supporto di uno staff multietnico e di un team di mediatori culturali che dialogano costantemente con le comunità immigrate. I nostri clienti si fidano: siamo noi a scegliere a seconda della comunità immagini colori e linguaggio differenti. Inoltre produciamo Mixità, newsletter che racconta consumi, stili di vita e curiosità degli stranieri che vivono in Italia».

la Repubblica

23-MAR-2018
pagina 19
foglio 1

Intervista

L'Agenzia digitale "Per la carta d'identità è illegale chiedere solo contanti"

JAIME D'ALESSANDRO, ROMA

Classe 1965, imprenditore nel campo del digitale, blogger e politico, è il presidente del comitato di indirizzo per l'Agenzia dell'Italia digitale dal 2014. Sospira e prova a mettere in fila le idee sui problemi che sono sorti a macchia di leopardo per la consegna della carta d'identità elettronica. Iniziando dai ritardi che a volte diventano biblici e dalla pretesa di alcuni uffici che pretendono il pagamento in contanti.

«Intanto una premessa: le pubbliche amministrazioni sono tenute per legge ad aderire al sistema di pagamento elettronico "pagoPA"».

Sta dicendo che chi obbliga al contante è fuori legge.

«Esatto. Ma non c'è sanzione. Non possiamo picchiare i dirigenti che non rispettano la legge.»

Picchiarli no. Però è fantozziano pretendere un pagamento in contanti nel 2018 e per di più per la carta di identità elettronica, quando la legge ti impone di accettare anche i pagamenti digitali.

«È vero: l'Italia è disomogenea nello sfruttamento della tecnologia per facilitare il rapporto fra uffici pubblici e cittadini. Il comitato strategico dell'Agenzia per l'Italia digitale, con il Team per la Trasformazione digitale, sta facendo un lavoro grosso per cercare di spingere le amministrazioni verso il piano strategico triennale che abbiamo disegnato. Guardiamo la parte positiva: è la prima volta che abbiamo una strategia e che abbiamo un piano».

Però poi succede quel che succede.

«Bisogna spingere sull'acceleratore per colmare le disomogeneità. Non significa spendere di più, ma trasmettere più determinazione. A Milano la maggior parte delle pratiche le svolgono in digitale. Ci sono gli strumenti e ci sono anche le leggi. Abbiamo perfino istituito la figura del responsabile della trasformazione digitale. Ministeri, comuni, tutte le pubbliche amministrazioni lo devono avere e serve proprio a implementare le innovazioni. Ma a volte non viene nemmeno nominato. E così un'amministrazione è eccellente e l'altra no. È una questione in parte culturale».

Ecco. Che però va superata.

«Per quanto riguarda l'eIdas ("electronic IDentification", serie di norme europee che riguardano l'identificazione elettronica, *ndr*) noi siamo all'avanguardia assieme alla Germania. Ora però servirebbe decisione da parte della politica nell'obbligare ad adottare le norme e le leggi che già abbiamo. E in futuro servirebbe anche un commissione parlamentare per l'innovazione che si occupi solo di questo e un ministero come lo hanno tanti Paesi. Magari sul modello di quello di Taiwan che invece di avere un suo gabinetto ne ha uno formato dai dirigenti degli altri ministeri. È una sorta di coordinamento fatto dai vertici ministeriali che poi riportano alle varie amministrazioni. In questo modo non c'è un'entità sperata che guarda al futuro, ma è parte della macchina esistente».

Stefano Quintarelli Cinquantadue anni, imprenditore nel campo del digitale, blogger e politico (parlamentare di Scelta civica nella legislatura da poco conclusa), Stefano Quintarelli è dal 2014 presidente del Comitato d'indirizzo dell'Agenzia per l'Italia digitale, ente pubblico nato per favorire l'innovazione tecnologica nella pubblica amministrazione

Il Messaggero

23-MAR-2018
pagina 1
foglio 1 / 2

L'Europa e Pechino

L'occasione di ridisegnare il commercio mondiale

Giulio Sapelli

Gli Stati Uniti hanno esportato sicurezza e crescita economica nel corso di circa quarant'anni: quelli della guerra fredda con l'ex Unione Sovietica. Caduto il muro di Berlino gli americani sono stati gli alfieri della globalizzazione. Ma la globalizzazione è stata in larga parte un gioco di specchi. L'unica merce veramente globalizzata è stata la moneta e il capitale come flusso e non come investimento.

Il fiume della finanza circolava e circola in un letto pieno di scogli, paracarri, dighe e tutto travolge inarrestabilmente dopo le decisioni angloamericane della fine degli anni ottanta del Novecento (presidenza Clinton e premierato Blair) di sregolare i mercati finanziari e di privatizzare le banche abolendo la distinzione tra banche d'affari e banche commerciali e dando così vita alla finanza distruttrice dei derivati e delle collateralizzazioni dei debiti. Il tutto mentre, per decisione di Bill Clinton, e quindi della finanza sregolatrice che governa la classe politica americana con un sistema lobbystico unico al mondo, si è consentito alla Cina di entrare nel Wto senza di fatto nessuna contropartita.

Le conseguenze sono state terribili. Il mondo è stato invaso da merci a bassissimo contenuto di valore e ad alta aliquota di distruzione dell'ambiente e della sostenibilità.
La deindustrializzazione era l'inevitabile conseguenza di questa inaudita misura dettata solo dall'interesse finanziario e speculativo dei manager occupati solo a massimizzare il valore delle loro stock option e delle grandi banche d' affari. Si sono così poste le basi per la distruzione della stessa potenza americana. I dati del commercio mondiale sugli scambi tra Stati Uniti e Cina sono eloquenti e implacabili. La Cina è il primo partner commerciale degli Stati Uniti, con un terribile sbilanciamento a favore di Pechino: nel 2017 il commercio bilaterale ha raggiunto i 636 miliardi di dollari, con 130 miliardi di dollari di esportazioni americane e 506 miliardi di importazioni, con un surplus di 376 miliardi a favore di Pechino. Donald Trump è determinato a ridurre tale squilibrio usando come argomento la minaccia alla sicurezza nazionale e la violazione della proprietà intellettuale attraverso massicci trasferimenti di tecnologie americane alle élite belliciste cinesi. Nel frattempo, per anni, l'Unione europea si è incartata in un'inutile discussione sul se definire o meno quella cinese una economia di mercato. E adesso teme le misure di Trump che sono invece dirette a difendere anche la stessa Europa che si è privata nel tempo di quell'esile protezionismo selettivo che ne caratterizzò gli inizi fondativi, quando la cultura industriale prevaleva su quella finanziaria e speculativa.

Ora tra le classi dominanti e tra la tecnocrazia europea, sempre più oligarchicamente protesa a un liberismo amministrato dall'alto delle procedure e lontano dalla sana competizione tra imprese, si diffonde la paura e l'angoscia dinanzi all'attivismo neo protezionistico positivo di Trump e altro non si sa fare che battere i pugni e minacciare ritorsioni, dimenticando che l'Europa non può fare a meno degli Stati Uniti. E in ogni caso cooperare con l'America è meglio che competere dinanzi all'aggressività cinese. Gli Stati Uniti hanno iniziato minacciando dazi sull'acciaio. L'Europa ha strillato senza mai dire ciò che noi italiani abbiamo detto invece sin da subito con Antonio Gozzi, presidente di Federacciai . Ossia che il pericolo che ne deriva per l' Europa e per l'Italia da quei dazi scaturisce dal fatto che l'acciaio che rimbalza contro gli scudi nord americani finirebbe in Europa, danneggiando forse per sempre la nostra industria. Da un lato si ignora la concorrenza fraudolenta dell'acciaio cinese ed asiatico, dall'altro ci si preoccupa solo di chiedere l'esenzione

Il Messaggero

23-MAR-2018
pagina 1
foglio 2 / 2

della Unione europea dalle misure nord americane. Sarebbe questo invece il momento di cogliere l'occasione per ridefinire tutta la politica mondiale doganale e del commercio approfittando del salutare scossone che Trump ha dato a un sistema insostenibile e che a lungo andare potrebbe portare alla distruzione vera e propria non solo dell'industria, ma dello stesso sistema sociale occidentale. È bene che si prenda atto che in questa nuova partita il nemico è la Cina. L'Europa deve capirlo prima che sia troppo tardi.

Avvenire
23-MAR-2018
pagina 4
foglio 1 / 2

Startupper africani sui banchi della Bocconi

Venti giovani imprenditori a Milano per formarsi e incontrare investitori internazionali

Sono attivi nei settori più diversi, dall'agricoltura alla logistica, dalla, telesanità alla mobilità elettrica

CATERINA MACONI

Una settimana di corsi intensivi di imprenditorialità allo Sda Bocconi school of management, al termine dei quali incontrano venture capitalist europei potenziali finanziatori.

È l'esperienza che hanno fatto venti giovani imprenditori provenienti dall'Africa, a Milano, a marzo, grazie a un'iniziativa di Sda Bocconi for growth. Per molti di loro è stato il primo viaggio in Europa. Si tratta di una iniziativa pro-bono: coperte le spese di viaggio, il soggiorno e la formazione a Milano, gli startupper hanno seguito per cinque giorni un corso coordinato da Mikkel Draebye, docente di entrepreneurship in Bocconi. Al termine del quale hanno partecipato al "Bocconi & Africa 2018. Forum on Entrepreneurship", la tre giorni sull'Africa organizzata dall'ateneo, culminata per loro con lo Startup Day - Special Focus on Africa, l'incontro con venture capital e business angels internazionali in cerca di nuove opportunità in cui investire.

Come sono stati selezionati i 20 candidati? Fanno parte dei 5mila partecipanti al progetto Adansonia, promosso sempre da Bocconi con lo scopo di insegnare attraverso un corso online di 6 settimane a dare forma alla propria idea di business. I migliori sono stati invitati in Italia dopo una selezione da parte di una commissione formata da professionisti africani ed europei sulla base dei migliori business plan.

«Sda Bocconi for growth è il progetto di Sda Bocconi school of management che ogni anno, dal 2012, mette a disposizione gratuitamente la propria conoscenza e il lavoro di docenti e personale per aiutare la crescita di persone, imprese o organizzazioni che sono o si sono trovate in condizioni di difficoltà», spiega Giuseppe Soda di Sda Bocconi. Negli anni scorsi a beneficiarne sono state per esempio imprese colpite dal terremoto, rifugiati, disabili. «Abbiamo scelto l'Africa perché se ne parla sempre come Paese fonte di problemi più che di opportunità – prosegue Soda –. Crediamo che lo sviluppo passi da una generazione di giovani in grado di creare imprese sostenibili. Vorremmo ripetere l'esperienza il prossimo anno, continuando a concentrarci sul continente africano, che crediamo sia il continente del futuro».

I 20 imprenditori provengono da Camerun, Uganda, Ghana, Kenya, Nigeria, Senegal e Sudafrica. Sono attivi nei settori più diversi, come agricoltura, logistica, immobiliare, telesanità, mobilità elettrica, media, fino alle app che favoriscono l'incontro tra domanda e offerta in settori come i trasporti e le riparazioni delle auto.


L'Africa punta a crescere con la sua moneta unica

Startupper africani sui banchi della Bocconi

Avvenire
23-MAR-2018
pagina 4
foglio 2 / 2

le esperienze

Matovu/Uganda

«Portiamo il pagamento mobile nelle aree rurali del Paese»

Charles Matovu è attivo in Uganda con Amac Ltd. È una startup che ha un triplice obiettivo: progetta, produce e commercializza eco-bag per la vendita al dettaglio; fornisce servizi e soluzioni per il pagamento mobile nelle aree rurali e ha progetti nell'ecoturismo per turisti africani. «Abbiamo iniziato a ottobre 2016 – spiega Matovu – ora sono impiegate 5 persone, di cui 3 full time» e sono legati a gruppi di donne che lavorano sul territorio.


Charles Matovu

«La nostra sede è a Kyegwa Town Council, nella sottoregione di Rwenzori nell'Uganda occidentale», precisa. È un giovane imprenditore di 36 anni ed è la prima volta che viaggia fuori dai confini africani. Si dice entusiasta di essere a Milano e di questa esperienza (e ci tiene a precisare che è la prima volta che vede la neve). Ai business angel ha parlato delle eco-bag state pensate come mezzo per fornire confezioni alternative ai sacchetti di politene. Ma anche dell' e-commerce, dove «forniamo servizi di pubblica utilità e proponiamo modalità di pagamento tramite cellulare mobile nelle aree rurali». Poi c'è l'aspetto turistico, per ora con focus su vacanzieri africani. Qui «prestiamo servizi di alloggio per i turisti e organizziamo performance art attraverso spettacoli di intrattenimento culturale. Vendiamo, inoltre, a turisti e altri clienti locali, presso la nostra sede nella città di Kyegegwa, prodotti artistici e artigianali realizzati da associazioni di donne e di giovani». **(C.Mac.)**

Bih/Camerun

«Il nostro network immobiliare per costruire case sostenibili»

In Camerun la 35enne Tim Immaculate Bih è dal 2017 il ceo di "Butterfly Housing Camerun". Un progetto in fieri che è la «joint venture tra una società di costruzioni con sede in Camerun e una società con sede nei Paesi Bassi», racconta. Di più: la volontà è quella di formare un network in diversi Paesi del continente, e infatti sono già state aperte sedi in Sud Africa e Nigeria. Obiettivo: costruire case sostenibili e a basso costo per il mercato locale, che sta crescendo molto.


Tim Immaculate Bih

«Sono entusiasta di essere qui», dice Bih. Il Camerun è un Paese dalle enormi potenzialità per il mercato immobiliare, «ma è difficilmente servito. Esiste un grande divario tra domanda e offerta», prosegue. Loro sono attivi con abitazioni sostenibili «che aiutano a ridurre l'utilizzo di energia». Il governo del Camerun ha stimato che nei prossimi dieci anni sarà necessario costruire 1 milione di case per andare incontro alla necessità della popolazione.

Butterfly Housing Camerun offre diversi tipi di case con un design comune, destinate a chi cerca soluzioni convenienti e sostenibili e ha un reddito basso o medio. Sono basate su un sistema di costruzione ibrido: consiste in strutture in acciaio che sono assemblate insieme in quello che costituisce lo scheletro della casa. Completano il tutto altre componenti come pannelli isolanti e materiali locali. Il risultato sono case sostenibili che creano posti di lavoro sul territorio. **(C.Mac.)**

Il Sole 24 ORE
23-MAR-2018
pagina 1
foglio 1 / 2

FOCUS. L'IMPATTO DEI TWEET SUI LISTINI

Così il «cinguettio» dei robot manipola le news sui titoli

INCHIESTA

I tweet dei robot insidiano così le news dei listini

RICERCA ITALIANA

Negli Usa i titoli minori citati «ad arte» insieme ai big. Obiettivo? Farli entrare nel radar dei trader automatici

di **Vittorio Carlini**

Basta un tweet! Un «cinguettio» per manipolare l'informazione dei mercati. Soprattutto se, nel mondo dei social network, a «gorgheggiare» non è un uomo. Bensì un robot. La riprova? La fornisce una ricerca, realizzata all'interno del progetto UE SoBigData, da un gruppo di scienziati italiani. Gli esperti hanno analizzato 9 milioni di tweet, lanciati sul social network tra maggio e settembre scorsi, in cui si discuteva di azioni quotate sulle principali Borse americane.La serie storica dei dati sui titoli (30.032 società) è stata, poi, incrociata con le informazioni finanziarie di Google Finance riguardanti le aziende stesse.

Ebbene: è saltato fuori un quadro molto interessante e, per alcuni aspetti, inquietante. «Ci siamo accorti -spiega Fabrizio Lillo, coautore della ricerca e professore di matematica per l'economia e la finanza all'Università di Bologna - della presenza di rilevanti anomalie».

Vale a dire? «In molti tweet, che riguardavano importanti società del Nasdaq o del Nyse, erano citati altri titoli di minore valore». Cioè: le cosiddette penny-stock, quotate su mercati non regolamentati, caratterizzate spesso da basse capitalizzazioni e scarsi volumi.

«Orbene - aggiunge Lillo - l'anomalia che abbiamo più volte notato è che, senza una reale giustificazione, tutto ad un tratto questi tweet venivano re-tweettati moltissime volte e in pochissimo tempo».

Un andamento anomalo che ha incuriosito il pool di esperti (composto da Stefano Cresci, Serena Tardelli e Marizio Tesconi del CNR di Pisa oltre che da Daniele Regoli della Scuola Normale di Pisa).

Gli scienziati, sfruttando un sofisticato algoritmo in grado di "smascherare" gli account fittizi, si sono resi conto che il boom dei re-tweet era opera di robot. Sembrerà incredibile ma la "valanga" di rilanci del «cinguettio» era realizzata da algoritmi. Una dinamica che, evidentemente, può in ipotesi concretizzare la manipolazione dell'informazione sui mercati finanziari nei social network. «Lo scopo - conclude Lillo - evidentemente è di rendere "interessante" la penny-stock agganciandola a dei titoli più noti».

Già, agganciare azioni meno rilevanti a titoli maggiormente "importanti". Ma a quale fine? Un'ipotesi molto gettonata tra gli operatori di mercato, a ben vedere, è quella di sfruttare l'ecosistema iper-tecnologico delle Borse stesse.

Vediamo di spiegarci. I listini, soprattutto negli Stati Uniti, sono attraversati in lungo e in largo da trader automatici. Sistemi che, tra le diverse variabili, monitorano costantemente i flussi di informazioni in arrivo dai social network. Si tratta, spesso, di meccanismi di intelligenza artificiale in grado di sfruttare i cambiamenti di "umore" degli stessi social. È chiaro che, nel momento in cui c'è il picco di re-tweet, l'*Artificial intelligence* segnala il mutamento. Un cambio di "sentiment" che, ecco il perchè del link con titoli più importanti, non sarebbe quasi mai percepito rispetto alle azioni minori.

Al contrario: la citazione del penny-stock, nel «cinguettio» che riguarda il titolo monitorato dall'intelligenza artificiale, può consentire all'azione stessa di entrare nel radar dei trader automatici. I quali, in ipotesi, possono prendere posizione su di un'informazione che, però, è sbagliata. Modificata, per l'appunto, dai robot che hanno realizzato i migliaia di re-tweet.

Fantafinanza? Tutt'altro. Diverse ricerche hanno dimostrato l'influenza dei social network e dei siti Internet sugli stessi prezzi delle azioni. Può ricordarsi, in tal senso, l'esperimento in cui è stato messo a confronto il *sentiment*, legato alle notizie pubblicate dal portale Yahoo! Finance, con l'andamento delle azioni cui le news erano riferite. Ebbene: da solo il *sentiment*, è risultato avere scarsa rilevanza. Diverso, invece, il discorso con l'utilizzo di un'ulteriore variabile: il numero dei click, fornito dal portale stesso, alla notizia in oggetto. Ebbene, in questo caso il carattere "predittivo" del *sentiment*, cioè di anticipare l'andamento del prezzo dell'azione, è aumentato di parecchio. Insomma: la Grande Rete, in tutte le sue articolazioni, ha da tempo un'in-

Il Sole 24 ORE

23-MAR-2018
pagina 1
foglio 2 / 2

fluenza notevole rispetto alle dinamiche di Borsa.

Una situazione che, da una parte, può dare luogo a manipolazioni ed abusi. E, dall'altra, richiede maggior pressing da parte delle autorità di controllo dei mercati.

Lo sviluppo delle tecnologie in finanza, di là dal tema dei social, oltre a innegabili benefici ha creato non pochi problemi. Negli Usa, proprio di recente, la Commissione di controllo dei future sulle commodity (Cftc), insieme al Dipartimento di giustizia e l'Fbi, ha multato tre banche e diversi trader per avere avere manipolato il mercato sfruttando lo "spoofing". Una strategia, tipica dei flash trader, che consiste nell'immettere un ampio flusso di proposte di negoziazione, tramite piattaforme computerizzate, sui listini. L'obiettivo? Non quello di concludere l'operazione, bensì di creare una fittizia informazione sul mercato stesso. Di nuovo: si manipola il mercato tramite la tecnologia.

LA PAROLA CHIAVE

Penny stock

● Le «penny stock» sono azioni di aziende vicino alla bancarotta, con un prezzo corrente prossimo allo zero. Tipicamente un titolo penny stock si muove in laterale e con bassa volatilità per molto tempo, per poi avere improvvisamente forti accelerazioni di prezzo sia al rialzo che al ribasso. Questo genere di titoli accelera quindi la propria volatilità sulla base di notizie estemporanee: sono dunque oggetto di speculazione nella previsione di un improvvisa impennata, positiva o negativa, delle quotazioni.

Il "peso" dei Tweet

La fotografia dei dati analizzati dalla ricerca nei mercati Usa

	Compagnie	Utenti	Tweet	Retweet
NASDAQ	3.013	252.587	4.017.158	1.017.138 (25%)
NYSE	2.997	265.618	4.410.201	923.123 (21%)
NYSEARCA	726	56.101	298.445	157.101 (53%)
NYSEMKT	340	22.614	196.545	63.944 (33%)
OTCMKTS	22.956	64.628	584.169	446.293 (76%)

Fonte: studio Progetto Ue SoBigData

Il Sole 24 ORE

23-MAR-2018
pagina 1
foglio 1

STRATEGIE PER IL WEB

INTERNET E MONOPOLI

Serve il coraggio dello Sherman Act

di **Marco Onado**

L'ammissione di responsabilità da parte di Zuckenberg dopo un lungo, imbarazzato silenzio apre una nuova fase nello scandalo che ha coinvolto Facebook e che ha avuto un grande impatto nell'opinione pubblica, ma che era nell'aria. Non occorreva essere addetti ai lavori per intuire le incognite e i rischi di reti di informazione che sono capaci di entrare nei dettagli più minuti della nostra vita privata, in modi che Orwell non avrebbe potuto immaginare mentre scriveva del Grande Fratello in *1984*.

Tanto che da tempo i nuovi grandi protagonisti della tecnologia sono stati definiti con l'acronimo di BAADD, *bad, addictive, anti-competitive and destructive to democracy*. Forse una generalizzazione eccessiva, ma anche un modo efficace per mostrare i rischi della grande svolta tecnologica che stiamo vivendo e che muta radicalmente molti dei parametri tradizionali nel modo di operare delle imprese. In primo luogo quello delle dimensioni dei partecipanti e dunque del ruolo possibile della concorrenza, da sempre fattore di equilibrio per eccellenza. Nella nuova realtà, la dimensione cresce esponenzialmente su sé stessa proprio per la capacità delle imprese di utilizzare le informazioni sui consumatori, per l'interesse dei venditori a usare quella piattaforma (è il motivo per cui Amazon ha ormai quasi la metà del mercato delle vendite online in America) o per il desiderio degli utenti di far parte di una comunità sempre più grande. Proprio Facebook, con i suoi due miliardi di contatti al mese, oscura tutti gli altri media tradizionali messi assieme. Ma soprattutto sono cambiate radicalmente le determinanti della catena del valore industriale. Facebook è diventata una delle prime società al mondo per capitalizzazione grazie alle informazioni che forniamo sulle nostre preferenze e i nostri gusti attraverso messaggi e indicazioni apparentemente innocenti come "mi piace" o "non mi piace". Gli utenti spensierati e felici sono in realtà i produttori ignari del valore. La via al profitto segue cioè regole profondamente diverse da quelle dell'economia tradizionale: è tutta basata sulla tecnologia (Facebook investe in R&S somme enormi) che consente di massimizzare la diffusione a milioni di seguaci e dunque la platea di fornitori di informazioni. Infatti l'intuizione geniale di Zuckenberg, come spiega bene il film "The social network" è stata quella di trasformare una rete ad uso esclusivo degli studenti di Harvard in un fenomeno planetario. Le regole ovviamente ci sono, tanto che sin dal 2011 Facebook aveva raggiunto un accordo ventennale con la potente Federal Trade Commission americana sulla protezione della privacy degli utilizzatori e oggi rischia grosso perché se si accertasse una violazione agli impegni presi le sanzioni sarebbero molto pesanti. Anche l'Europa si accinge a varare una nuova regolamentazione sulla protezione dei dati molto severa almeno sulla carta. Nuove regole sulla privacy e controllori dotati di armi efficaci sono ovviamente la condizione necessaria per proteggere non solo il funzionamento del libero mercato ma anche le basi essenziali del processo democratico. Ma forse non sufficiente perché si tratterebbe comunque di una risposta puramente quantitativa, cioè del potenziamento di mezzi tradizionali rispetto ad una realtà che è mutata nella sua stessa natura. Come in tutte le grandi svolte economiche della storia, si liberano energie positive, ma anche negative e il mondo delle regole deve dimostrare di essere in grado di compiere un salto di qualità adeguato alla nuova realtà. La rivoluzione industriale ha prodotto un grande balzo in avanti della produzione, ma anche inquinamento, sfruttamento, monopolio. Sia pure a caro prezzo e grazie alla presa di coscienza dei lavoratori, le nazioni industriali hanno saputo dare una risposta ai nuovi problemi, difendendo i diritti, spezzando i monopoli e varando leggi generali (si pensi alle leggi bancarie dopo la crisi degli anni Trenta negli Stati Uniti e in Europa) che affrontavano alla radice i problemi del settore, non – come è invece è stato fatto adesso – mettendo un cerotto su ogni specifico punto di crisi.

Proprio qui sta il nocciolo del problema. La capacità di esprimere riforme di ampio respiro all'altezza dei problemi da affrontare richiede una politica alta e indipendente. Fin dagli albori della rivoluzione industriale, i governi hanno risposto alle pressioni dal basso con riforme di ampio respiro. L'America ha saputo combattere il lato oscuro dei capitani dell'industria e della finanza che hanno guidato lo straordinario sviluppo dell'Ottocento, fino al punto di definirli Robber Barons. Oggi è completamente diverso, come è dimostrato dallo stupore con cui milioni di utenti stanno prendendo coscienza del fatto di essere non solo utenti, ma produttori di informazioni e valore. Per non parlare del fatto che tanti politici di oggi (forse proprio a cominciare da Trump) devono la loro elezione all'uso non corretto di dati. Le grandi riforme nascono dalla buona politica e questo richiede grande consapevolezza e capacità critica degli elettori. Ci sarà un motivo se perfino l'FT titola un suo pezzo: «utilizzatori di reti sociali di tutto il mondo, unitevi!».

Il Messaggero

23-MAR-2018
pagina 8
foglio 1

L'intervista Oreste Pollicino

«Posseggono i nostri dati e li conservano per sempre»

IL PROFESSORE DELLA BOCCONI: CHI DETIENE QUESTE INFORMAZIONI MANIPOLA LA POLITICA

Oreste Pollicino, professore alla Bocconi di diritto dei media, lei ha fatto parte del gruppo di esperti della Commissione europea sulle fake news. La vicenda di Cambrigde Analytica è un salto di qualità nei tentativi di manipolazione del consenso?

«Qualcosa di simile lo avevamo già visto con le elezioni americane. C'è un report del Dipartimento di giustizia che dimostra come un'agenzia russa abbia veicolato false notizie presso elettori statunitensi per influenzare le elezioni».

Colpisce la facilità con la quale è possibile acquisire dati di milioni di persone.

«I dati, da quello che è emerso fino ad oggi sono stati acquisiti in modo legittimo, attraverso una app per un test psicologico. Tra l'altro non ci sono irregolarità, almeno inizialmente, nemmeno nei rapporti tra Facebook e Cambridge Analityca, tanto è vero che quando la stessa Facebook si è accorta dell'utilizzo dei dati da parte della società di marketing politico, ha bloccato l'applicazione ed ha chiesto la distruzione dei dati. Credo che il problema sia un altro».

Quale?

«La conservazione dei dati. Queste informazioni una volta raccolte, per quanto tempo vengono conservate? E a che fini?».

Perché è importante?

«Perché prima si pensava che i dati venissero raccolti sostanzialmente per un solo scopo: quello di profilare i clienti a fini pubblicitari. Poi negli anni scorsi si è aggiunto un altro scopo: quello della sicurezza contro il terrorismo. Adesso abbiamo scoperto questo terzo filone della conservazione dei dati, legato alla dimensione politica. È inquietante».

Cosa spaventa di più?

«La possibilità di utilizzare le informazioni per manipolare l'opinione pubblica. Fino ad oggi il dato personale era rimasto in un'area di irrilevanza politica. Il dato utilizzabile per questi fini è un cambio di paradigma allarmante. Anche più delle fake news».

Sulla privacy nonostante tutto, c'è un sistema di regole che non riesce a proteggere. Come mai?

«Perché le regole sono sempre scritte per fronteggiare le situazioni patologiche: cosa succede se c'è una violazione. Come dimostra questo caso serve la prevenzione, che non passa per il diritto, ma per l'informatica. Servono misure di sicurezza preventive per evitare questi danni».

Chi dovrebbe essere a investire in prevenzione, la stessa Facebook, che in realtà sembra aver chiuso più di un occhio?

«Non demonizzerei Facebook. Un tema centrale rimane quello che il consenso degli utenti deve essere sempre più informato. Non ci si può accontentare di sapere che si fa un test psicologico, ma bisogna conoscere anche i fini per i quali le informazioni vengono raccolte. Serve trasparenza. I motivi per i quali vengono acquisiti i dati sono alla base delle regole del loro trattamento. Questa è stata la grande falla dimostrata dal caso Cambridge».

Andrea Bassi

il Fatto Quotidiano
23-MAR-2018
pagina 8
foglio 1 / 2

Allarmismi Le campagne politiche come le pubblicità. Le informazioni da sole non servono

Dal clic alle urne? Non proprio. Viaggio nella filiera dei dati

L'INCHIESTA

Il meccanismo "Targettizzare" richiede uno sforzo produttivo enorme. L'Italia, ad esempio, non ce l'ha

» VIRGINIA DELLA SALA

Dati rubati, profilati, sottratti: la politica italiana è diventata improvvisamente esperta di privacy. Aizza le masse, chiede alla vigilanza di vigilare, alle procure di indagare. Condanna genericamente l'uso dei dati social per la propaganda politica. Come se esistesse un nesso causa - effetto automatico tra un contenuto elettorale o una fake news e il voto nelle urne, come se avere i dati di 50 milioni di americani garantisce 50 milioni di voti per Trump (o per la Lega). Ma le cose non stanno proprio così. E in Italia, non c'è questo rischio.

IL TECNICO. "Qui è impossibile che sia stato utilizzato il metodo di Cambridge Analytica. E se anche fosse, l'esito delle elezioni non sarebbe cambiato". Dino Amenduni è un comunicatore politico e pianificatore strategico di Proforma, agenzia di comunicazione di Bari che ha curato le campagne del Pd. Parte da una premessa: il dato di cui si parla tanto non corrisponde a un nome e un cognome. Non è personale. È un identikit con associate caratteristiche sociodemografiche che, eventualmente, possono essere incrociate con la navigazione. Esempio: 30 anni, milanese, maschio, ha messo "mi piace" alla pagina di tizio. Questo dato arriva nelle mani di Cambridge Analytica. Che però usa anche il modello psicografico. Il dato in sé, infatti, non basta per la propaganda. Serve un modello per l'utilizzo. Quello elaborato da Cambridge Analytica è basato su uno studio accademico del 2012 che incrociava lo stile di navigazione degli utenti su Facebook, con i tratti di personalità estrapolati da un test diffuso sul social network. Incrociando i due elementi si potevano fare delle previsioni: una persona affetta da nevrosi potrebbe essere più sensibile a un messaggio che incuta paura. "Non esistono però evidenze scientifiche che dimostrino la correlazione diretta tra l'esposizione a un messaggio e il voto. Bisogna ragionare sul funzionamento della propaganda". Diversa infatti è la combinazione tra l'esposizione a messaggi veicolati con la psicografia e il vissuto personale. "Se vedo un messaggio che mi dice che i migranti sono cattivi e poi vedo un bus pieno di migranti allora potrei pensare che quel messaggio sia verosimile - dice Amenduni - Ma senza il contesto, il messaggio non serve a nulla". Il metodo potrebbe essere stato utile quindi solo negli Stati dove Trump ha vinto per pochi voti. "Non a New York, per dire".

La pianificazione social è prevista in tutte le campagne elettorali con lo stesso metodo delle pubblicità: messaggi personalizzati tramite inserzioni microtarghettizzate di Facebook. In media in Italia valgono il 15% del budget.

Parliamo con uno dei social media manager di ISayData, società che in passato ha curato l'immagine web di alcuni politici, tra cui Ignazio Marino o Gianni Cuperlo. "L'uso dei dati non è negativo - spiega - . Ricevere campagne personalizzate evita di essere inondati da quelle inutili". Sostiene che siano più efficienti di quelle tradizionali. I contenuti sui social possono essere monitorati con più facilità, osservando le interazioni. "Studiando le reazioni si può capire come hanno votato.

Ma come funziona la filiera? Si elabora un contenuto, lo si carica nella sezione delle inserzioni di Facebook e si indica il pubblico di riferimento. Il social permette un estremo livello di personalizzazione. Non puoi arrivare a dire voglio parlare con Tizio a meno che non ti abbia dato il suo indirizzo di posta (perché si può creare un pubblico personalizzato) ma, per dire, si può decidere che arrivi a tutte le persone che


Nuove accuse per Facebook Ora in Italia indagano i pm

Dal clic alle urne? Non proprio. Viaggio nella filiera dei dati

il Fatto Quotidiano
23-MAR-2018
pagina 8
foglio 2 / 2

hanno 30 anni, donne, sposate, interessate alla politica, ai cani, all'allattamento al seno, che abbiano N amici, che siano legati a una pagina Facebook e non a un'altra. Nulla di straordinario. Lo si fa per la pubblicità e anche per la politica. Basta pagare. Il costo.Dipende dalla durata dell'inserzione, dal pubblico e dai destinatari. Più è grande il pubblico più servono soldi. Più è piccolo più servono soldi: targettizzare l'audience aumenta il prezzo.

VARIA anche in base al numero di inserzioni online contemporaneamente su un determinato territorio o segmento sociodemografico. Se tutti vogliono parlare con i 35enni residenti in Wisconsin durante le elezioni, allora il costo aumenta. "Costa però infinitamente meno rispetto ai media tradizionali - spiega Amenduni -. Uno spot per il Super Bowl costa 5 milioni di dollari. Con la stessa cifra Trump sui social può campare per mesi". E infatti ha speso 5 milioni per Cambridge Analytica.

E la psicologia? Riguarda anche la creatività di chi pensa la campagna. Il team di Trump ha sviluppato decine di migliaia di messaggi diversi al giorno per personalizzarli il più possibile. "L'attività per far fruttare quella mole di dati è spaventosa - dice Amenduni - In Italia non saremmo in grado di produrre una cosa del genere. I budget per le campagne stanno pure diminuendo".

La scheda

ONLINE
Si elabora un contenuto, lo si carica nella sezione delle inserzioni di Facebook e si indica con precisione il pubblico di riferimento. Il social permette un estremo livello di personalizzazione

IL COSTO
Dipende dalla durata dell'inserzione, il pubblico e i destinatari. Più è grande il pubblico più servono soldi. Più è targettizzato maggiore è il prezzo. Varia anche in base alle inserzioni che ci sono online con quei parametri

ItaliaOggi
23-MAR-2018
pagina 2
foglio 1

IL PUNTO

Chi ci offre un servizio gratis è uno che si appresta a fregarci

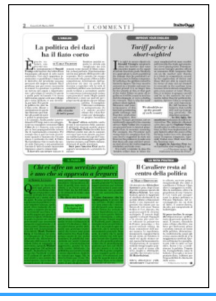
Questa infatti è la logica dei social network

DI SERGIO LUCIANO

Quando lo facciamo, cioè ogni giorno, non ce ne rendiamo conto, ma acconsentire a che il social network dove stiamo navigando usi i nostri dati è da pazzi. È come permettere a qualcuno di prenderci le misure corporee (altezza, spalle, punto vita) credendo che sia un sarto, e scoprire che invece ci sta facendo una bara. E ci fa anche pagare per questo. È questa la ragione di fondo per la quale, in queste ore, sta imperversando una sacrosanta tempesta reputazionale e di Borsa contro i Mammasantissima del web. Innanzitutto il detestabile **Mark Zuckerberg**, il brufoloso inventore-trafugatore di Facebook (piuttosto che difendersi in tribunale dall'accusa di aver rubato l'idea ai compagni di università, i gemelli **Winkelvoss**, pagò loro 180 milioni di dollari). Zuckerberg ha permesso che Facebook vendesse 51 milioni di «profili» dei suoi utenti a una società che, notoriamente, viveva facendo manipolazioni di comunicazione politica, la Cambridge Analytica. Cinquantuno milioni di profili sono tanti; se riferiti a un Paese come gli Stati Uniti che ha 330 milioni di abitanti in totale sono tantissimi.

Ma dove sta la sorpresa? Facebook e gli altri social media vivono esattamente di questo! Ci chiedono i dati, e noi glieli diamo perché altrimenti non possiamo usare i social, che invece sono parte della nostra vita. E poi li adoperano contro di noi: anche mandarci la pubblicità concentrata sui nostri interessi è un uso concettualmente aggressivo, perché fa leva sulle nostre debolezze. La pubblicità asseverativa tende a creare dipendenze. Andrebbe vietata per legge. Ma (si dirà) lo fanno per vivere. No, non vivere: per straguadagnare. E poi: chi glielo chiede di offrirci tutto in modalità pseudo-gratuita? Ci facciano pagare qualcosa, poi vedremo se continueremo a usare compulsivamente una quantità di servizi sostanzialmente inutili!

Come Amazon: che ha raddoppiato il prezzo del suo servizio «Prime» perché si è resa conto che i suoi costi altrimenti sono insostenibili. Prima ha cercato di creare dipendenza nei suoi clienti verso questo fattorinaggio velocissimo, e adesso alza il prezzo. Sempre meglio di Facebook, però: almeno, le consegne sono un servizio reale. Ma è un modo di agire deplorevole, che il mercato sta severamente punendo. Sono anni, in realtà, che le poche menti critiche sul web spiegano invano che il gratis non esiste e che quando qualcuno ci dice che fa gratuitamente qualcosa per noi, nel 99,9% dei casi mente e ci sta fregando. Ma la gente semplice, cioè la maggior parte di noi, a questi avvertimenti non crede fin quando non ci sbatte il muso. Ecco, ce lo stiamo sbattendo: ed era ora.



LA NOTIZIA
GIORNALE.IT
23-MAR-2018
pagina 6
foglio 1 / 3

Il Far West della rete

NON SOLO FACEBOOK ALTRI POTERI FORTI CI SUCCHIANO I DATI

> STEFANO SANSONETTI

Non solo Cambridge Analytica. Anche altri centri di potere stanno rastrellando dati dai social network a fini commerciali, civili e militari. Lo rivela a *La Notizia* l'ex capo degli specialisti informatici delle Fiamme Gialle, Umberto Rapetto. Nel frattempo l'Italia prepara un'Authority per la cyber security, stanziando però solo spiccioli.

CON INTERVISTA A UMBERTO RAPETTO ALLE PAGINE 6 E 7

Altri poteri forti succhiano dati Gli utenti ora devono frenarsi

Rapetto: Facebook è solo la punta dell'iceberg E le Autorità italiane sono le uniche a non muoversi

Il quadro

Per l'ex numero uno degli specialisti delle Fiamme Gialle è in corso un rastrellamento di informazioni online

di **STEFANO SANSONETTI**

Ciò che non si è fatto prima non si può fare certo adesso, con l'epidemia ormai scoppiata e del tutto incontrollabile. Anche perché non c'è solo Cambridge Analytica interessata a fare man bassa di dati prelevati dai social network, da utilizzare poi ai fini più vari, da quelli politici a quelli commerciali. Al punto che l'unica soluzione possibile, ora, è quella di "togliere benzina alla macchina", ovvero "insegnare alla gente a mettere un freno alla voglia esibizionistica di esternare particolari della propria vita". A usare queste parole è **Umberto Rapetto**, già generale della Guardia di Finanza, fondatore del Gat delle Fiamme Gialle, il primo gruppo anticrimine tecnologico. Rapetto, considerato uno dei massimi esperti italiani di minacce informatiche, ha poi abbandonato la Guardia di finanza (non senza qualche polemica), per passare a Telecom e infine mettersi in proprio. Sullo scandalo dei dati carpiti a Facebook, non si sa con quanta complicità da parte del social network, ha le idee molto chiare.

Generale, siamo a un punto di non ritorno?

LA NOTIZIA GIORNALE.IT
23-MAR-2018
pagina 6
foglio 2 / 3

"Siamo solo alla punta dell'iceberg, altri sicuramente ammetteranno di aver debordato nel rastrellare a fini commerciali e politici i dati degli utenti dei social".

Faccia qualche nome.

"Inutile fare nomi, visto che si tratta di numerose coalizioni di interessi politici, commerciali, militari che trovano estrema facilità nella raccolta di questi dati. Del resto le regole di Facebook per i singoli utenti sono di centinaia di pagine incontrollabili, mentre quelle per i partner commerciali lasciano spazio a tutto ciò che non è espressamente vietato. Ma ciò che non è vietato è talmente vago da regalare enormi margini d'azione"

Sì, ma provi a dire cosa farebbe lei oggi se fosse a capo del Governo.

"Guardi, al punto in cui siamo l'unico modo di reagire è togliere benzina alla macchina. Intendo dire che gran parte della colpa è nostra, che non riusciamo a tenere a freno l'esibizionismo e la voglia di condividere dati della nostra vita. Bisogna insegnare alla gente a darsi un freno. Certo, per quanto riguarda l'Italia registro una totale latitanza delle Autorità. Nel Regno Unito e negli Stati Uniti sono partite convocazioni a raffica, a volte anche con toni draconiani. Da noi invece non si è mossa foglia".

In questi giorni in Parlamento (vuoto per il cambio di legislatura) è arrivato il decreto che attua la direttiva europea "Nis", quella sulla sicurezza delle reti e dei sistemi informativi. C'è qualche intuizione spendibile?

"Non mi faccia parlare del decreto, per carità".

Cioè?

"Provvedimento del tutto inutile, che rimette a palazzo Chigi la lotta alle minacce cibernetiche. Ma che c'entra palazzo Chigi? L'intelligence in tema di cyber security compete al ministero della Difesa, come succede negli altri Paesi. Se invece parliamo di ricerca e sviluppo l'Italia dovrebbe dotarsi di un vero think tank governativo. Invece noi abbiamo tutta una serie di fondazioni tematiche il cui unico scopo è quello che raccattare soldi a destra e sinistra per vivere.

Il decreto stanzia 3 milioni l'anno per le nuove strutture deputate alla sicurezza informatica. Non sono un po' poche?

"È la prova dell'incompetenza con cui si è trattata la faccenda".

LA NOTIZIA GIORNALE.IT
23-MAR-2018
pagina 7
foglio 1 / 2

Cyber security all'italiana Una nuova Authority ma con pochi spiccioli

Nuovo team costituito a Palazzo Chigi Risorse e sanzioni a dir poco esigue

L'ultima novità

L'organismo si chiama Csirt e dovrà lavorare con cinque ministeri Il tutto utilizzando solo 3 milioni l'anno

di **STEFANO SANSONETTI**

Una strategia a tre teste, ma al momento con pochi spiccioli a disposizione. Mentre impazza lo scandalo Facebook, con una valanga di dati di utenti utilizzati a fini politici dalla società Cambridge Analytica, sul più vasto tema della cyber security l'Italia sta cercando di approntare la sua risposta. Il tutto in attuazione di una direttiva Ue di cui si discute da anni, quella sulla "sicurezza delle reti e dei sistemi informativi". Uno degli ultimi atti del Governo guidato da **Paolo Gentiloni** è stato proprio la predisposizione di un decreto legislativo di attuazione del provvedimento europeo, che paradossalmente giace inerme proprio in queste ore presso le competenti commissioni di Camera e Senato. In attesa che un Parlamento operativo possa dare i relativi pareri (in teoria la scadenza è prevista per il 2 aprile), è interessante andare a leggere lo schema che da qui alla fine del 2018 dovrà prendere corpo. La strategia prevede tre nuclei di controllo sulla sicurezza di reti e sistemi informatici. Si parte con la definizione delle cosiddette Autorità Nis (Network and Information Security), deputate all'applicazione delle nuove norme. Il decreto italiano, suddividendole in settori di competenza, le identifica in cinque ministeri: Sviluppo economico (competente per energia, gas, petrolio e servizi digitali), Infrastrutture (aerei, ferrovie e vie d'acqua), Economia (banche e mercati finanziari), Salute (operatori di assistenza sanitaria) e Ambiente (operatori della distribuzione dell'acqua pubblica). Ebbene, l'articolo 10 del decreto legislativo stabilisce che entro il 9 novembre del 2018 questi cinque Ministeri (come detto nella veste di autentiche Autorità di controllo) dovranno identificare per ciascun settore di competenza "gli operatori di servizi essenziali con sede sul territorio nazionale". L'operazione è necessaria all'istituzione, presso il Ministero dello Sviluppo, di un elenco di operatori di servizi essenziali, da aggiornare ogni due anni. A facilitare l'identikit di questi operatori è un allegato al decreto, dal quale si desume che tutte le società come Eni, Enel, Terna, Snam, Ferrovie, aziende di trasporto areo, Autorità portuali, banche, ospedali (pubblici o privati) dovranno essere inserite nell'elenco. Accanto a esse ci dovranno essere anche operatori di "mercato on line" (leggasi Amazon), "motori di ricerca" (Google) e servizi di cloud computing (qui si fa un riferimento alla Sogei, la società informatica del Tesoro). Insomma, nella lista dovranno esserci tutte realtà che operano sulla base di reti e sistemi informatici. L'altra testa dello schema è la costituzione di un nuovo organismo presso la Presidenza del Consiglio, ovvero il Csirt (Computer security incident response team). Si tratta, precisano le relazioni tecniche, di una "struttura tecnico-operativa di prevenzione e trattamento degli incidenti informatici". L'articolo 8 del decreto spiega che potrà essere composto al massimo da 30 membri, 15 dei quali scelti tra i dipendenti della Pa (in co-

LA NOTIZIA GIORNALE.IT
23-MAR-2018
pagina 7
foglio 2 / 2

mando o fuori ruolo) e 15 provenienti dall'esterno. Il Csirt, che erediterà funzioni simili a quelle svolte dagli attuali Cert, è un po' il cuore del meccanismo. A questo team, infatti, tutti gli operatori registrati nell'elenco dello Sviluppo economico dovranno far pervenire, "senza ingiustificato ritardo", le segnalazioni di incidenti aventi un impatto rilevante. La terza gamba del meccanismo, nel ruolo di coordinamento con le altre Autorità europee, c'è il cosiddetto "punto di contatto unico", che il decreto identifica nel Dis, ovvero il Dipartimento che coordina i nostri servizi segreti. Insomma, come si vede il piano è particolarmente elaborato.

A CORTO DI DENARO

Semmai a far riflettere è l'esiguità delle risorse messe in campo per sostenerlo. Gli oneri per far fronte all'attività delle Autorità Nis (i cinque ministeri) e del Csirt (il team di reazione e gestione degli incidenti informatici) vengono fissate in 5 milioni di euro nel 2018, che poi scendono a 3 milioni l'anno a partire dal 2019. Così come esile appare l'apparato sanzionatorio che dovrebbe convincere gli operatori iscritti nell'elenco dello Sviluppo a collaborare puntualmente con lo stesso Csirt. L'articolo 21 del decreto, a seconda del tipo di mancanza accertata, delinea multe che vanno da un minimo di 12mila a un massimo di 120mila euro, oppure da un minimo di 25mila a un massimo di 125mila euro. Non proprio un "siluro" per i colossi energetici o digitali. Ma i numeri sono modesti soprattutto se si considera che in Italia, nel 2017, oltre 16 milioni di utenti della rete sono "caduti in trappole informatiche" con conseguenti perdite economiche per circa 3,5 miliardi di euro (come ha rivelato il "2017 Norton Cyber Security Insight Report"). Da segnalare, infine, che il decreto non si applica alle società di telecomunicazioni, che rientrano nei controlli previsti dal Codice delle comunicazioni elettroniche.

Carissime trappole informatiche Nell'ultimo anno in Italia danni per 3,5 miliardi di euro

Ormai è una piaga. Ma l'altra faccia della medaglia è che parliamo di una frontiera di business crescente. Il fenomeno ha assunto dimensioni tali che anche l'ultimo decreto del Governo Gentiloni, che prova a dare attuazione alla direttiva europea sulla sicurezza delle reti e dei sistemi informativi, si affida a report internazionali per ragionare su dati aggiornati. Nelle schede tecniche allegate al provvedimento si premette che il contesto internazionale è molto variegato: "a fronte di Paesi nei quali le problematiche di cyber security sono state affrontate già da tempo in modo strutturato, esistono invece situazioni nelle quali invece le politiche in materia non si sono ancora sviluppate in modo adeguato". Solo nel 2017 "i numerosi attacchi informatici hanno causato danni economici per un importo pari a 146,3 miliardi di euro a 978 milioni di utenti di 20 Paesi (secondo il "2017 Norton Cyber Security Insight Report"). Anche in Italia, proseguono le stesse schede tecniche, gli incidenti di cybersicurezza causano ingenti danni alle imprese e ai cittadini. Nel 2017 oltre 16 milioni di utenti della rete sono "caduti in trappole informatiche" con conseguenti perdite economiche per circa 3,5 miliardi di euro (sempre secondo il "2017 Norton Cyber Security Insight Report"). Come si vede, un caos enorme.

SPOT A RISCHIO

Le agenzie britanniche minacciano di mollare Zuckerberg & Co.

Gli inserzionisti britannici minacciano di abbandonare Facebook dopo la vicenda del sospetto abuso dei dati di decine di milioni di utenti. E' quanto è emerso ieri da una riunione dell'Isba, l'organismo che rappresenta le maggiori agenzie pubblicitarie del Regno, il cui messaggio - a quanto ha riferito la *Bbc* - è "il troppo è troppo". David Kershaw, boss del colosso M&C Saatchi, ha confermato poi che la minaccia di passare su altre piattaforme "non è un bluff" in mancanza di garanzia di svolte sulla sicurezza dei dati. Facebook, dal canto suo, ha smentito la voce, riferita nei giorni scorsi dal New York Times, secondo cui il capo della sicurezza del social, Alex Stamos, avrebbe lasciato il suo ruolo. Di sicuro sul caso i prossimi giorni non potranno che riservare altre sorprese.

Economy
IL BUSINESS MAGAZINE DI MONDADORI
01-APR-2018
pagina 32
foglio 1 / 2

GESTIRE L'IMPRESA

Ecco la nuova privacy che va trattata con i guanti bianchi

Garantire il trattamento dei soli dati personali necessari ad una specifica finalità e assicurare massima sicurezza in caso di violazioni: ecco il perchè del GDPR

di Riccardo Venturi

Secondo uno studio condotto da IDC, solo il 3% delle aziende con più di 10 dipendenti si è già adeguato al nuovo Regolamento generale sulla protezione dei dati. Il 54% ha un piano già predisposto, ma il 43% è solo all'inizio della fase di analisi... Una situazione che migliora tra le banche, già soggette a un'authority e più avvezze a questo tipo di regole, ma che peggiora ulteriormente tra le imprese di altri settori come il commercio e i servizi. Tante aziende italiane che pure gestiscono dati personali, insomma, hanno fatto trascorrere i due anni di fase transitoria prima dell'entrata in vigore della GDPR senza attrezzarsi, svolgendo poca o nessuna formazione al proposito. Un ritardo che potrebbe costare caro, viste le multe salatissime previste dal nuovo regolamento. Ancora oggi non sembra esserci un'adeguata consapevolezza del fatto che le novità non comportano solo cambiamenti di carattere informatico e burocratico, ma anche e soprattutto organizzativo. Non è quindi così semplice capire come gestire l'adeguamento alla nuova normativa, specie quando alla sua entrata in vigore mancano ormai solo poche settimane. «La GDPR, a differenza della normativa precedente, è risk based - spiega ancora Fabrizio Bulgarelli, Head of RAS e IT Services di RSM, ma anche coautore della norma UNI 11697 che definisce i profili professionali relativi al trattamento e alla protezione dei dati personali in ambito GDPR - questo significa che per alcuni tipi di dati si deve fare un'analisi del rischio, una prassi più vicina alla cultura anglosassone, che non ci è familiare». La valutazione d'impatto è in particolare obbligatoria nei casi di trattamento con rischi elevati per i diritti delle persone fisiche; introduzione di un nuovo servizio, sistema informativo o nuova tecnologia, o modifiche di processi e procedure; trattamento dei dati sensibili e giudiziari; trattamenti su larga scala. Un altro cambiamento portato dalla GDPR è il concetto di privacy by default, che ha anche delle implicazioni importanti di carattere tecnologico: «chi non ha un motivo oggettivo di accedere ai dati non lo potrà più fare, e le nuove procedure devono essere disegnate facendo un'analisi preventiva dei rischi, e in qualche caso chiedendo l'autorizzazione al garante per effettuare trattamenti completamente automatizzati» aggiunge Bulgarelli. Per questo, il titolare del trattamento dei dati mette in atto misure tecniche e organizzative adeguate volte ad attuare in modo efficace i principi di protezione dei dati, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del regolamento e tutelare i diritti degli interessati. Si vuole così garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Questo, beninteso, tenendo conto dello stato dell'arte, dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, sia al momento di determinare i mezzi con i quali lo si svolge sia all'atto del trattamento stesso. Alla privacy by default la GDPR aggiunge quindi la privacy by design: la protezione dei dati deve essere parte integrante della stessa progettazione dei processi aziendali. Il che si ricollega al tema della valutazione dell'impatto, la PIA (Private Impact Analysis): «Un errore che fanno in tan-

TANTE AZIENDE CHE GESTISCONO DATI PERSONALI HANNO FATTO PASSARE I 2 ANNI DI FASE TRANSITORIA SENZA ATTREZZARSI E FORMARSI SUL GDPR

Economy
IL BUSINESS MAGAZINE DI MONDADORI
01-APR-2018
pagina 32
foglio 2 / 2

Prevenzione da:
- Furto di identità
- Usurpazione identità
- Perdite finanziarie
- Danni alla reputazione
- Perdita segreto professionale
- Danni fisici
- Danni materiali
- Danni immateriali
- Limitazione diritti dell'individuo
- Danni economici
- Danni sociali

ti è non lavorare sulla selettività della privacy: non tutti i dati personali hanno la stessa importanza. Per essere sicuro di minimizzare il rischio di non-compliance devo insomma saper fare una selezione dei dati su cui c'è un rischio alto» puntualizza Fabrizio Bulgarelli. Le principali fasi del lavoro che porta alla stesura di un report completo di PIA sono la definizione dei criteri di rischio (fattori legali, business...), l'identificazione dei processi e sistemi da valutare ai fini dei rischi per la privacy, la redazione di un piano per il trattamento dei rischi e la selezione dei controlli da implementare. Altro elemento chiave del nuovo Regolamento è quello che rivoluziona gli obblighi delle aziende in caso di furto dei dati, il temuto "data breach" che collega il tema della privacy a quello della cybersecurity. Le aziende infatti saranno tenute a comunicare la violazione entro 72 ore (!) al Garante dei dati personali e al cliente se c'è un rischio per lui molto significativo. Un obbligo da non prendere sottogamba, visto che si rischiano multe fino a 20 milioni di euro. Meglio quindi non far finta di niente, come pure in passato è successo in diverse occasioni anche a realtà non piccole. Più nel dettaglio, il titolare del trattamento notifica la violazione riguardante la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati all'autorità di controllo competente ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza e deve: descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione; comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni; descrivere le probabili conseguenze della violazione dei dati personali; descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi. Vista la complessità del nuovo regolamento, la prossimità della sua entrata in vigore, le multe previste, può essere saggio affidarsi a chi conosce bene la materia e sa come muoversi anche in tempi ridotti. «Seguiamo tutto il percorso di adeguamento aziendale alla GDPR, inclusa la scelta del DPO, la realizzazione del modello organizzativo, la segmentazione per aree aziendali – dice l'esperto di RSM, società leader internazionale nei servizi di Audit, Consulting, Tax & Legal - In mancanza di una fase transitoria, che ormai è alle spalle, aiutiamo le aziende a capire rapidamente cosa c'è da fare in termini informatici e organizzativi, adottando un approccio differenziato tra i large account, con la fornitura di componenti informatiche per gestire tutti i processi, e il middle market, per il quale utilizziamo un approccio integrato con il modello di organizzazione e gestione della 231, che permette di migliorare la governance a costi sostenibili». La caratteristica dell'approccio di RSM alla gestione del nuovo Regolamento generale sulla protezione dei dati è la sistematicità. Il lavoro viene svolto in maniera integrata su tutti gli aspetti coinvolti, dalla parte legal a quella informatica, da quella organizzativa agli strumenti a supporto della privacy, fino all'automazione dei processi. La metodologia utilizzata è il GICS, GDPR Integrated Compliance Solution, un approccio supportato da una piattaforma tecnologica modulare integrata sviluppata da RSM e dai partners. Una soluzione agile e scalabile, che può essere completamente fornita anche come servizio in modalità cloud. «Con questo approccio, che mi piace definire olistico, siamo anche in grado di riutilizzare il lavoro già svolto per le norme precedenti, compatibile con la GDPR» conclude Bulgarelli.

PER LE IMPRESE, L'UNICA VIA PER METTERSI IN REGOLA PER TEMPO È AFFIDARSI A CHI CONOSCE LA MATERIA E IL REGOLAMENTO IN OGNI ASPETTO

Economy
IL BUSINESS MAGAZINE DI MONDADORI
01-APR-2018
pagina 31
foglio 1

PRIVACY E GDPR/COSA CAMBIA PER TUTTI DA MAGGIO

GDPR, PROTEGGI I NOSTRI DATI (E LIBERACI DALLE SANZIONI)

Tremano le aziende ancora impreparate all'imminente entrata in vigore del nuovo Regolamento. Ma non mancano le lacune normative, come ci spiega un membro del gruppo UE di sviluppo del nuovo codice

di Riccardo Venturi

Adeguarsi in fretta alla normativa per evitare multe tra il 2-4% del fatturato consolidato annuo. È l'imperativo categorico in vista dell'entrata in vigore il prossimo 25 maggio del GDPR (General Data Protection Regulation). Con il "Regolamento generale della protezione dati" che in Italia sostituirà il Codice della privacy, la Commissione europea intende rafforzare la protezione dei dati personali dei cittadini dell'UE. Imponendo alla Pubblica Amministrazione ealle imprese che gestiscono dati personali, incluse le Pmi, una serie di regole nuove e stringenti.

FABRIZIO BULGARELLI
PARTNER - HEAD OF RISK ADVISORY SERVICE (RAS) AND IT SERVICES RSM SOCIETÀ DI REVISIONE E ORGANIZZAZIONE CONTABILE S.P.A.

«Le aziende sono in difficoltà, perché il regime transitorio è alle spalle e non è stato sempre utilizzato per adeguarsi al nuovo regolamento – dice Fabrizio Bulgarelli di RSM – la difficoltà è comprendere quanto di quel che è già stato fatto sulla base delle norme precedenti possa essere valido per le nuove». Diverse le incombenze previste dal GDPR, a cominciare dal registro delle attività di trattamento, sorta di elenco dei dati personali oggetto della normativa, associati con le responsabilità organizzative e le misure di sicurezza correlate. Viene poi introdotta la nuova figura del responsabile della protezione dati (DPO, Data Protection Officer), obbligatoria quando il trattamento dati è effettuato da un'autorità o un organismo pubblico, e quando avviene su larga scala. Peccato che il regolamento non dia alcuna definizione di trattamento su larga scala.

«IL GRUPPO EX ART. 29, TRA GLI ESEMPI DI LARGA SCALA, INDICA IL TRATTAMENTO DATI DI GEOLOCALIZZAZIONE RACCOLTI SUI CLIENTI DI UN FAST FOOD GLOBALE»

Economy
IL BUSINESS MAGAZINE DI MONDADORI
01-APR-2018
pagina 34
foglio 1 / 2

ESCLUSIVO/Parla Antonello Soro
«Imprese, non sottovalutate le nuove regole. Non adeguarsi costerà assai più che farlo»

GESTIRE L'IMPRESA

PRIVACY, L'ALLARME DI SORO «LE IMPRESE SONO TROPPO DEBOLI NELLE DIFESE CONTRO GLI HACKER»

Intervista con il Garante della Privacy alla vigilia dell'entrata in vigore del nuovo regolamento ispirato dalla direttiva europea: «Le aziende si adeguino, le sanzioni sono poca cosa rispetto ai danni del cybercrime»

di Francesco Condoluci

"L'IDEA DI FONDO È CHE LA SOCIETÀ DIGITALE RICHIEDE REGOLAMENTAZIONI DIVERSE DA QUELLE PREESISTENTI. Perché fin quando il volto deteriore della digitalizzazione si limita ad un hackeraggio irritante ma innocuo della posta della segreteria, si può anche far spallucce. Ma quando, com'è capitato lo scorso anno ad una impresa britannica, l'hackeraggio determina un danno che è stato quantificato in 700 milioni di sterline, c'è poco da far finta di niente!": è molto chiaro Antonello Soro, presidente dell'Autorità Garante per la protezione dei dati personali. Sotto le finestre del suo spartanissimo ufficio di piazza Montecitorio a Roma sfilano mescolati indistintamente manifestanti e turisti, dal quarto piano i rumori si sentono appena ma è come se l'intero palazzo fosse circondato dall'infinito ronzio dei dati che gremiscono la rete, quei dati di tutti noi che migliaia di soggetti nel mondo possono carpire e usare a nostra insaputa. Una nuova regolamentazione europea, in vigore dal prossimo maggio (vedi Economy, numero 9) imporrà una brusca sterzata alle aziende, costringendole a presidiare con ben altro piglio i dati propri e soprattutto quelli dei propri clienti. E non mancano i mugugni contro le salatissime multe a carico di chi non si adeguerà. Ma adeguarsi è sacrosanto.

Presidente, spieghi lei perché...

I dati da proteggere non sono aride cifre ma sono le proiezioni delle nostre persone nella nuova dimensione della vita che è il digitale. I dati sono i protagonisti della società digitale, sono il nuovo petrolio dell'economia digitale, ma dal punto di vista giuridico sono l'oggetto di un diritto fondamentale della persona, e pertanto ne va garantita l'inviolabilità.

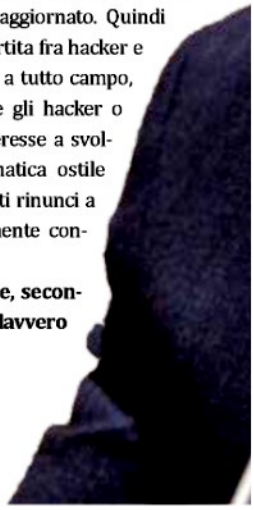
Chi ha interesse invece a violarli?

Gli hacker, una variabile non eludibile. Ci sono e vanno contrastati. Invece i sistemi di difesa delle imprese, non solo in Italia ma in tutto il mondo, sono di totale debolezza. Per questo mi auguro che le nuove regole inducano un cambio di atteggiamento delle imprese verso questo problema. La protezione dei dati non va considerata un costo ma una risorsa. Gli investimenti per proteggere il proprio patrimonio informativo sono fondamentali per la sicurezza, personale e aziendale, per la reputazione e in assenza di questi un'impresa rischia di essere devastata, con oneri ben più grandi del costo di un pacchetto di software aggiornato. Quindi il tema vero è: la partita fra hacker e impresa si giocherà a tutto campo, non illudiamoci che gli hacker o chiunque abbia interesse a svolgere attività informatica ostile verso imprese o Stati rinunci a farlo se non duramente contrastato.

LA PARTITA FRA HACKER E IMPRESE SI GIOCHERÀ A TUTTO CAMPO, NON ILLUDIAMOCI CHE RINUNCINO AI CRIMINI SE NON LI CONTRASTEREMO

Ma le nuove norme, secondo lei, potranno davvero essere efficaci?

LE NUOVE REGOLE SONO MOLTO EFFICACI E LA PORTABILITÀ DEI DATI È DECISIVA



Economy
IL BUSINESS MAGAZINE DI MONDADORI
01-APR-2018
pagina 34
foglio 2 / 2

Sì, la spiego meglio. Questo nuovo regolamento europeo è un primato dell'Unione nel mondo, perché si fa carico di dare risposte a problemi che pongono la protezione dei dati al centro dell'impegno. In un mondo frammentatissimo, l'Europa è riuscita a produrre con il regolamento un sistema di norme che tendono ad aggregare a legare allo stesso destino un territorio di 500 milioni di persone, con un sistema che è già un modello per Australia, Canada, India, Paesi sudamericani. Arrivando a uniformare per l'Europa a 27 più il Regno Unito le norme applicabili agli Ott (over the top: i colossi come Google e Facebook, ndr) in modo tale che la circolazione dei dati e l'accelerazione degli scambi avvenga in un contesto di sicurezza!

E l'efficacia?

C'è. Oltre alla protezione del dato dalle intrusioni di soggetti non autorizzati, abbiamo introdotto il diritto, complicatissimo da attuare ma fondamentale, della portabilità del dato. Ossia: i dati che ho deliberatamente affidato ad una qualsiasi piattaforma restano miei e solo miei e potrò in ogni momento riprendermeli come faccio col il mio numero di telefono. Una misura che non è solo una grande tutela per il cittadino, ma è anche, e fondamentalmente, uno strumento di contrasto ai continui comportamenti anticoncorrenziali, per cui oggi le imprese che hanno catturato un utente tendono a non mollarlo mai... E non basta.

Cos'altro?

All'articolo 22 il nuovo regolamento stabilisce che nessuna decisione significativa per un individuo può essere presa esclusivamente in base a un trattamento automatizzato dei suoi dati. E' concettualmente una norma che circoscrive gli ambiti di applicazione della cosiddetta intelligenza artificiale.

Bene: ma chi garantirà tutto ciò?

Il regolamento istituisce una figura nuova, quella del responsabile della protezione dei dati, o data protection officer. E' un professionista dell'impresa, o dell'ufficio della pubblica amministrazione, che orienterà l'organizzazione dei sistemi di un'azienda affinchè sia la più adeguata per proteggere i dati ad essa affidati fungendo da tramite tra l'Autorità di protezione dati e il vertice aziendale.

VEDO ANCORA UN PO' DI AFFANNO IN GIRO, MA CREDO CI SIA STATO NEGLI ULTIMI MESI UN RECUPERO D'INIZIATIVA DA PARTE DEL SISTEMA ECONOMICO

E a quali funzioni sovrintenderà questo sceriffo aziendale?

In particolare, il responsabile della protezione dei dati si dovrà occupare di tutti i trattamenti svolti dall' azienda e dovrà supportare il titolare nell'adozione di tutte le misure tecnico-organizzative, , adeguate a prevenire rischi per i dati dei clienti, proteggendo i sistemi aziendali e tutto il patrimonio informativo. Le imprese, applicando il regolamento, non dovranno più fare richieste di verifiche preliminari al momento di realizzare nuovi prodotti o nuovi servizi, ma dovranno farsi carico di progettare sistemi sicuri e che riducano al minimo l'uso di dati e. Dovranno adottare sistemi di privacy by-design, come si dice in termini tecnici, caratterizzati cioè dall'incorporare nei prodotti e nei servizi fin dalla loro progettazione misure ad hoc per proteggerei dati dei clienti. Dovranno anche determinare tempi di conservazione dei dati adeguati alle finalità del trattamento e prevedere un sistema di accesso selettivo ai dati...

E veniamo all'Autorità: riuscirete a far fronte con le vostre risorse alle nuove incombenze di vigilanza sull'applicazione del regolamento?

Ci impegneremo a fondo. La nostra macchina è piccola ma molto efficiente. Dovremo crescere, ineluttabilmente. Questa autorità è stata calibrata per una società predigitale. Ora il Parlamento ci ha riconosciuto un aumento dell'organico. Siamo in 140, potremo acquisire altre 25 risorse. Si consideri che l'omologa autorità britannica conta 500 dipendenti e ne ha chiesti altri 200 per far fronte alle nuove incombenze. Faremo fronte stringendo i denti e facendo leva su una struttura qualitativamente all'avanguardia.

E le multe?

Trovo singolare che imprese accettino tranquillamente che per violazioni delle regole sulla concorrenza possano esserci sanzioni miliardarie e si indignino su quelle previste dalle violazioni contro le regole poste a tutela dei dati delle persone...

Un suo bilancio personale come Garante...

E' un ruolo molto faticoso ma molto interessante. Una finestra sul mondo con la 'emme' maiuscola, perché è un mondo dove c'è dentro di tutto. Ma soddisfa la curiosità intellettuale di chiunque. Per misurarsi col mondo, serve curiosità intellettuale. Del resto tutti avevamo sottovalutato la crescita vertiginosa dell'impatto dell'innovazione tecnologica sulla società. Arrivando qui, ho avuto un punto di vista privilegiato su questi temi.In fondo, questa società digitale che dobbiamo proteggere dagli hacker è lo sfondo su cui è cresciuta la nuova disciplina europea, che fronteggia la nuova geografia dei poteri, la nuova domanda di diritto e di riconoscimento dei diritti, le nuove incertezze della regolazione e della giurisdizione...

Un'ultima domanda: il sistema italiano è pronto?

Vedo ancora un po' di affanno in giro, ma credo ci sia stato negli ultimi mesi un recupero forte di iniziativa, prima da parte delle associazioni datoriali e delle Camere di Commercio e ora anche delle singole imprese...