

La sfida di Diego Piacentini sul digitale

L'articolo di Marco Mayer, docente di Cyberspace and International Relations alla Scuola Superiore Sant'Anna di Pisa

La rivoluzione digitale è un fenomeno globale, ma il suo impatto nei singoli paesi è fortemente differenziato. In alcune nazioni essa rappresenta un fattore di crescita e di benessere, in altre - al contrario - produce effetti negativi: perdita di competitività, emarginazione e declino.

In Italia la perdurante assenza di una politica pubblica digitale (*cyber public policy*)¹ sta producendo danni gravissimi nel breve e nel medio periodo. Il Paese da un lato rischia di subire tutte le conseguenze negative prodotte dai processi di digitalizzazione (soprattutto in termini di disoccupazione dei lavoratori con qualifiche di livello medio-basso).² Dall'altro corre il rischio di perdere la più rilevante opportunità di crescita di questo decennio (posti di lavoro qualificati in tutti i settori industriali e nei servizi, ricerca universitaria e privata, produzione di *know how*, imprese innovative e *startup*).³

Sintomo della debolezza italiana è il fatto che le grandi *major* digitali hanno in Italia quasi esclusivamente uffici commerciali, a differenza di quanto avviene in altri Paesi europei.⁴ La situazione è grave anche sul piano della sicurezza, dal momento che l'appropriazione indebita di brevetti, ricerche, prototipi, ecc. è cresciuta a livello esponenziale mettendo a repentaglio il patrimonio strategico/militare, industriale, tecnologico e scientifico italiano.⁵ La proprietà intellettuale del paese è quotidianamente soggetta ad una minaccia silente, ma a differenza di altri paesi tra i cittadini ed in vasti segmenti del mondo imprenditoriale, la sensibilità per la *cyber security awareness* resta tuttora molto scarsa.⁶

Crescita e sicurezza sono in realtà due facce della stessa medaglia, in quanto una strategia digitale competitiva e orientata allo sviluppo non può non comprendere una dimensione *security* caratterizzata dai più elevati standard internazionali. La *cyber security* è innanzitutto un'attività preventiva e pertanto dovrebbe essere "*embedded*" nei processi, nelle reti e in tutti i dispositivi.

Un ulteriore elemento di debolezza è costituito dalla spaventosa frammentazione che contraddistingue da anni il processo di digitalizzazione della PA. Un settore che in teoria potrebbe, invece, rappresentare - uno straordinario volano di crescita per il Sistema Paese. Il settore pubblico è diviso in tanti compartimenti stagni e la digitalizzazione "materiale" (spesso anche obsoleta) è stata sinora incapace di garantire interoperabilità tra le diverse amministrazioni centrali,⁷ tra lo Stato e le

autonomie territoriali, né un' efficace comunicazione tra autorità pubbliche, cittadini e imprese. Le stesse consistenti forniture pubbliche di servizi digitali (via Consip o senza Consip) sono la somma di esigenze settoriali - se non occasionali - e non hanno a monte un piano di riorganizzazione trasversale della PA capace di sfruttare in modo efficiente e creativo la vasta gamma di soluzioni offerte dalla rivoluzione digitale.

In numerosi casi – in assenza di un modello organizzativo ben definito – la digitalizzazione delle procedure pubbliche ha prodotto e tuttora sta producendo tragici effetti *boomerang*. Alcuni dei fenomeni più eclatanti – si pensi alla mera scannerizzazione del cartaceo - si sono verificati nei ministeri della pubblica istruzione e della sanità, per non parlare dell'arretratezza organizzativa e tecnologica di numerose ASL, Regioni ed enti locali.

Non si intendono qui negare alcuni progressi (fatturazione elettronica e ricettari medici digitali in alcune regioni virtuose, sperimentazione della carta di identità elettronica in qualche grande comune, ecc.),⁸ tuttavia la dispersione di energie e la frammentazione istituzionale sono ancora elevatissime, come peraltro ha dimostrato il dibattito parlamentare sull'emendamento Quintarelli in sede di riforma costituzionale (in questo caso un risultato politico positivo).⁹ La storica divaricazione tra Ministero degli Interni e Ministero dell'economia in materia di anagrafi -¹⁰ e l'ambiguità normativa e gestionale che in questi anni ha contraddistinto il ruolo e le attività dell'Agid - sono solo altri due esempi delle difficoltà esistenti.

In linea di principio, si potrebbe facilmente delineare una politica governativa, investimenti pubblici e una legislazione all'altezza delle nuove sfide, anche perché è oggi possibile far tesoro delle esperienze positive e negative di altri paesi.¹¹ Il punto centrale non è di *policy*, ma di *politics* (la *governance* in area Cyber, sicurezza compresa) e di comunicazione politica. La politica italiana dovrebbe riflettere sul fatto che la rivoluzione tecnologica non si limita a creare lo spazio cibernetico (il cosiddetto *cyberspace* o quinto dominio).¹²

E' l'intera realtà sociale e culturale che cambia; viviamo ormai in una vera e propria "società digitale" caratterizzata – a mio avviso - da cinque proprietà combinate ed inedite: iper-connettività a livello globale; iper-velocità della comunicazione; iper-memoria (miniere digitali o Big Data); iper-automazione dei processi (IOT); iper-capacità mimetica.

Quest'ultima caratteristica presenta giganteschi problemi di attribuzione non solo degli attacchi informatici, ma anche in termini di influenza dell'opinione pubblica e di manipolazione occulta del mercato.

La società digitale pone dunque in termini totalmente rinnovati la responsabilità politica dello Stato contemporaneo per quanto riguarda le politiche pubbliche, le strutture amministrative, i processi decisionali, i diritti civili e politici, la sicurezza ed i servizi al cittadino. Nella cultura della Silicon Valley i valori dominanti sono tecnologia e mercato, mentre la democrazia resta in ombra.¹³

Recenti studi hanno anche ipotizzato la presenza, all'interno delle società digitali, di un crescente grado di manipolazione politica (alcuni algoritmi nati per ragioni commerciali e pubblicitarie eserciterebbero – in termini preterintenzionali o per dolo - un'influenza di carattere politico). Si sostiene – ad esempio - che una percentuale crescente di elettori incerti sia influenzata, in termini subliminali e di persuasione occulta, dai motori di ricerca.

Due docenti statunitensi di psicologia, Robert Epstein e Ronald Robertson, hanno studiato i comportamenti dell'elettorato incerto in India e negli Stati Uniti ipotizzando che una consistente percentuale è inconsapevolmente influenzata dalle ricerche in internet. Epstein e Robertson hanno definito questo fenomeno con l'acronimo SEME (*search engine manipulation effect*).¹⁴ Questa ipotesi tuttavia è contrastata da opinioni opposte.¹⁵

Al di là della ricerca menzionata di cui è arduo verificare l'attendibilità - la verità è che non è affatto semplice conciliare i tempi, gli spazi e gli imperativi della società digitale con i valori fondanti delle democrazie contemporanee - un problema che rischia di aggravarsi ancor più ad ogni ulteriore balzo in avanti della tecnologia.

Su questo punto in Italia si registra un grave ritardo culturale e politico.¹⁶ Il tema è sostanzialmente assente dallo spazio pubblico; così come scarsa è la partecipazione delle università e delle imprese nazionali ai grandi appuntamenti internazionali sulla *governance* relativa al futuro di Internet e del *cyberspace*.¹⁷

In Italia, inoltre, sul piano della *politics* la molteplicità delle autorità politiche e tecniche deputate (Ministro dello sviluppo economico, Ministro della Funzione Pubblica, Interni, Difesa, altri ministeri, Regioni, ASL, Agid, altre agenzie, grandi comuni, ecc.) è in palese contrasto con la natura stessa della rivoluzione digitale. Per essere efficace tale rivoluzione richiede, infatti, la rottura dei compartimenti stagni e delle isole di potere (e delle relative gerarchie organizzative micro-settoriali). E' necessaria una visione trasversale e unitaria che consenta di agire con velocità, con una catena di comando chiara e secondo una logica net-centrica coerente con una visione a lungo termine dell'intero Sistema Paese.

Non vi è alcun dubbio che la politica digitale dell'Italia debba coinvolgere il Governo nel suo insieme e pertanto dipendere direttamente dalla responsabilità politica del Presidente del Consiglio ed, eventualmente, per delega da un suo Sottosegretario. Nel mondo cyber e nella realtà tecnologica contemporanea e futura non c'è spazio per l' "Italia dei dicasteri", per l' "Italia degli orticelli", per l' "Italia delle parrocchie e dei mille campanili".

In questa logica, l'autorità politica dovrà dotarsi di uno strumento in grado di attuare e concretizzare le priorità dell'agenda politica. Sotto questo profilo la Presidenza del Consiglio dovrebbe creare un nuovo Ufficio o un nuovo Dipartimento dedicato alla strategia ed alla politica digitale (*cyber public policy*), dotato di competenze adeguate sotto il profilo tecnico e di poteri effettivi sull'intera macchina centrale e periferica della PA.

Questa struttura non dovrebbe tuttavia rappresentare, come spesso è accaduto in Italia, un livello burocratico aggiuntivo teso a verificare adempimenti procedurali in chiave giuridico-legale. Se tale dovesse essere il rischio, sarebbe meglio abbandonare del tutto il progetto di una sua costituzione. Al contrario, si tratterebbe di realizzare una struttura capace di dare *input* strategici ed operativi e che risulti effettivamente competitiva a livello internazionale, in linea con gli altri Paesi industrializzati (non solo le grandi potenze, ma anche il Regno Unito, la Germania e la Francia, per non parlare di piccoli Paesi come Israele e l'Estonia dove i processi di digitalizzazione - *cyber security* compresa - costituiscono un rilevante fattore di crescita economica). In questa logica un altro aspetto cruciale riguarda la necessità di una radicale revisione legislativa ed organizzativa dell'Agid.¹⁸

Tuttavia, oltre al grave problema di *politics/governance*, esiste un altro aspetto critico di non facile soluzione, quello di una *comunicazione politica* decisamente fuorviante. Nella percezione di gran parte della classe politica, dei media e dell'opinione pubblica, la dimensione digitale è erroneamente associata a immagini effimere: al "gioco" dei *selfie* e dei cinguettii, al successo dei *social network* o comunque alla leggerezza del virtuale come se fosse un pianeta immaginario ed alieno dalla vita reale. Niente di più sbagliato. Queste cattive rappresentazioni nel mondo cyber sono solo la punta di un enorme *iceberg*.

La distinzione tra virtuale e reale non esiste più, se mai è esistita in precedenza. In ogni caso, siamo oggi di fronte ad una nuova e gigantesca "rivoluzione industriale" che ha riflessi dirompenti sulla vita di tutte le imprese, delle Pubblica Amministrazione e di ogni singolo cittadino (sia sul piano sia lavorativo che della vita privata). E' sbagliato pensare alla crisi economica come un effetto esclusivo

della crisi finanziaria, anche se essa ne ha costituito un rilevante acceleratore; la crisi è dovuta a un cambiamento sistemico in cui i modelli organizzativi aziendali, i prodotti, le metodologie di produzione stanno cambiando rapidamente.¹⁹ Di conseguenza, i paesi che vinceranno saranno quelli più sensibili a cogliere e gestire l'innovazione del digitale, i paesi che sapranno mantenere i propri cervelli e attrarne di nuovi.

La rivoluzione digitale ha inciso profondamente anche nelle dinamiche della politica internazionale. Il *cyberspace* è diventato a tutti gli effetti un elemento di *high politics*, un terreno di confronto/scontro tra le grandi potenze anche per la crescente convergenza e integrazione tra dimensione civile e militare.²⁰

Per queste ragioni è il momento di rompere gli indugi: occorre dotare l'Italia di una strategia, di una struttura di *governance* e di una capacità organizzativa all'altezza delle sfide della rivoluzione digitale.

Il 29 settembre scorso il Governo Renzi ha nominato Diego Piacentini (già numero due di Amazon) Commissario Straordinario per il Digitale.²¹ Gli obiettivi politici annunciati da Piacentini dopo la nomina sono ambiziosi e condivisibili:

*“rendere più semplice la vita ai cittadini... far sì che la macchina dello Stato sia in grado di usare le tecnologie come accade in Gran Bretagna e negli Stati Uniti....”*²²

Vedremo tra qualche mese se avrà una visione lungimirante, le idee chiare e soprattutto l'influenza necessaria per favorire il *catch up* dell'Italia. In bocca al lupo!

¹ Si veda Mayer, M. <http://www.ictsecuritymagazine.com/articoli/gli-imperativi-del-governo-italiano-per-la-cyber-security/>

² Carl Benedikt Frey e Michael A. Osborne della Oxford Martin School hanno esaminato 702 profili professionali nel mercato del lavoro degli Stati Uniti e sono giunti alla conclusione che il 47 % dei posti di lavoro è a rischio per effetto della rivoluzione digitale. Frey, C.B, Osborne, M..A The Future of Employment - Oxford Martin School, 2013. La Banca mondiale ha successivamente utilizzato la metodologia adottata dai due studiosi per una ricerca di carattere mondiale ed ha confermato il fenomeno a livello globale. Chi intende approfondire il tema può fare riferimento a lavori successivi. http://www.oxfordmartin.ox.ac.uk/downloads/reports/Citi_GPS_Technology_Work.pdf; <http://voxeu.org/article/how-digital-revolution-reshaping-global-workforce>

³Il 7 ottobre 2016 Cyber Affairs - l'agenzia di stampa diretta da Michele Pierrri - riporta la seguente dichiarazione di Lorenzo Mazzei (cyber security advisory leader di EY): “Il ritardo digitale” ci costa due punti del Pil e la mancata creazione di circa 700 mila posti di lavoro.” http://www.askanews.it/cyber-affairs/cyber-security-che-cosa-si-e-detto-a-ey-capri-2016_711912855.htm

⁴ Con la nuova eccezione della Apple a Napoli che, tuttavia, è limitata alla formazione di sviluppatori di *app*, ma non alla ricerca e innovazione: <http://www.corriere.it/italia-digitale/notizie/apre-apple-academy-napoli-seicento-nuovi-sviluppatori-app-81242492-8ba3-11e6-8000-f6407e3c703c.shtml>, un altro esempio recente è il distretto promosso dalla giapponese NTT data in Calabria

dedicato allo sviluppo e implementazione di soluzioni per la cyber security. NTT data:

<http://www.quotidianodelsud.it/calabria/economia/2016/10/07/assunzioni-cyber-security-colosso-ntt-data-assume-150-persone-cosenza>

⁵ Il Direttore del DIS- Prefetto Alessandro Pansa - ha recentemente ricordato: “... Nel dicembre 2014, Nomisma ha pubblicato gli esiti di uno studio, commissionato dal DIS, volto a valutare il livello di percezione della minaccia cibernetica nelle piccole e medie imprese... al fine di accrescerne la sicurezza informatica. Benché tale ricerca sia stata pubblicata ormai quasi un paio di anni fa, i relativi risultati possono essere purtroppo ritenuti ancora oggi validi”. <http://www.sicurezza nazionale.gov.it/sisr.nsf/archivio-notizie/pansa-per-litalia-un-progetto-forte-di-cybersecurity.html>. Il tema è anche al centro del libro bianco elaborato dal CINI (a cura di Baldoni. R, De Nicola R.) <https://www.consortio-cini.it/index.php/it/labcs-home/libro-bianco>

⁶ Tra le molteplici iniziative promosse dai governi segnaliamo questo progetto statunitense promosso dal Homeland Security Department: <https://www.dhs.gov/publication/stopthinkconnect-industry-resources>

⁷ Le difficoltà esistenti nonché l'esigenza di realizzare un coordinamento efficace tra le amministrazioni centrali sono esplicitate nella direttiva emanata il 1 agosto 2015 dal Presidente del Consiglio Matteo Renzi: <http://www.sicurezza nazionale.gov.it/sisr.nsf/archivio-notizie/la-sicurezza-del-cyberspazio-come-priorita-strategica.html>

⁸ Uno dei tanti esempi paradigmatici su cui riflettere è il fatto che nella prima fase sperimentale (2015) la dichiarazione dei redditi pre-compilata non aveva incluso le detrazioni sanitarie!

⁹ Se la riforma costituzionale verrà confermata dal referendum del 4 dicembre la dimensione informativa-digitale sarà materia d'interesse nazionale e dunque di competenza dello Stato. <http://www.polisblog.it/post/296498/emendamento-quintarelli-pubblica-amministrazione-digitalizzazione>

¹⁰ Basti pensare alle annose diatribe che hanno accompagnato il progetto, poi arenatosi, del cosiddetto “documento digitale unificato”. La previsione normativa è stata, infatti, abrogata nell'agosto 2015. Si veda: http://www.agendadigitale.eu/egov/53_le-tante-incognite-del-documento-digitale-unificato.htm, <http://www.ilsole24ore.com/art/norme-e-tributi/2013-09-18/dopo-anni-flop-nasce-111538.shtml?uid=Ab6CZ2XI&fromSearch>, <https://www.key4biz.it/carta-didentita-elettronica-non-decolla-da-13-anni-ma-il-governo-rilancia/138978/>, <http://serviziodemografici.interno.it/sites/default/files/Circolare%20n.%2010%20-%202016.pdf>,

¹¹ A livello internazionale il caso di maggiore successo è Israele. 7 anni fa una felice combinazione tra la visione lungimirante del Prof. Ben Isaac Israel dell'Università di Tel Aviv e l'intuito politico del primo ministro Benjamin Netanyahu hanno prodotto una strategia onnicomprensiva e vincente sul piano digitale. La storia è raccontata in un recente volume: Isaac Ben Israel, I. Tabansky, L. Cybersecurity in Israel, <http://www.springer.com/us/book/9783319189857>. L'università di Tel Aviv – su impulso della Farnesina ha anche stabilito una fattiva cooperazione con l'Università di Modena (il Centro diretto dal Prof. Michele Colajanni). <http://formiche.net/2015/09/28/le-sfide-della-cyber-security-viste-italia-israele/>. Anche Leonardo Finmeccanica ha stabilito degli accordi significativi con realtà israeliane. Tuttavia sarebbe sbagliato – come qualcuno ha suggerito - copiare il modello israeliano. Israele è un contesto del tutto particolare: si tratta un paese in guerra e nel quale le forze armate (IDF) hanno un ruolo primario al di là dei compiti strettamente militari.

¹² Nel 2014 in un lavoro presentato al MIT insieme a Fabio Ruggie ho illustrato la metafora del *cyberspace* in questi termini: “*Reframing K. Waltz images: cyber arena as a mirror that reflects the real world and at the same time it affects it*”. L'idea cioè che il *cyberspace* sia uno specchio “speciale” che non solo riflette il mondo reale, ma anche interagisce con esso influenzandolo. <http://ecir.mit.edu/images/stories/Images/Conference2014/Folder/workshopreportFINAL3.pdf>, p. 68. Tuttavia questa immagine – pur valida per descrivere il *cyberspace* in senso stretto - offre una visione parziale perché la distinzione tra virtuale e reale è estremamente labile.

¹³ Si è molto discusso di democrazia digitale, ma i risultati sono stati sinora deludenti. Si veda, tra le numerose pubblicazioni critiche il volume “il Mito della democrazia digitale” del Professor Matthew Hindman: <http://press.princeton.edu/titles/8781.html>.

¹⁴ “*The search engine manipulation effect (SEME) and its possible impact on the outcomes of elections*”: <http://www.pnas.org/content/112/33/E4512.full.pdf?with-ds=yes>, <https://aeon.co/essays/how-the-internet-flips-elections-and-alters-our-thoughts>, <https://www.wired.com/2015/08/googles-search-algorithm-steal-presidency/>

¹⁵ Si veda: <http://www.politico.com/magazine/story/2015/08/google-2016-election-121766>,
<https://www.theguardian.com/technology/2014/may/15/google-did-not-rig-indian-elections>, http://www.huffingtonpost.com/dr-robert-epstein/googles-hypocrisy_b_8253332.html

¹⁶ Per la verità la Casaleggio Associati già nel 2004 aveva intuito la centralità politica della rete (vedi il rapporto: focus politica online: https://www.casaleggio.it/wp-content/uploads/2014/11/Focus_politica_online_1.0.pdf. Il movimento Cinquestelle è stato peraltro l'unico movimento politico italiano capace di sfruttare le grandi potenzialità di Internet per la conquista di elettori. Viceversa per quanto attiene alla democrazia interna le consultazioni degli oltre 150.000 iscritti non pare aver inciso in profondità sugli esiti dei processi decisionali del movimento.

¹⁷ Per esempio nel congresso degli Stati Uniti si contesta ancora il progetto di eliminare il controllo americano su ICAAN (la struttura che assegna e gestisce tutti i dati anagrafici, i domini e gli indirizzi di Internet ed i relativi protocolli). Si veda: "*Should the U.S. Relinquish Its Authority Over the Internet Domain Name System?*", *CRS Insight*, October 5, 2016 <https://www.fas.org/sfp/crs/misc/R44022.pdf>.

¹⁸ Si tratta di ridefinirne le funzioni tecniche in modo da assicurare un fattivo rapporto tra pubblico e privato, uno stretto collegamento tra crescita dell'economia digitale, una nuova organizzazione industriale e la cyber security; nonché la capacità di promuovere iniziative adeguate alla crescita della cultura digitale e della sicurezza cibernetica, cominciando da quelle mirate ad elevare la consapevolezza del rischio (vedi nota 6).

¹⁹ Di notevole interesse in questo ambito è il lavoro di McKinsey sui processi di automazione relative alle tipologie di lavori: <http://www.mckinsey.com/business-functions/business-technology/our-insights/where-machines-could-replace-humans-and-where-they-cant-yet>, <https://public.tableau.com/profile/mckinsey.analytics#!/vizhome/AutomationBySector/WhereMachinesCanReplaceHumans>, <http://www.mckinsey.com/~media/McKinsey/Business%20Functions/Business%20Technology/Our%20Insights/Where%20machines%20could%20replace%20humans%20and%20where%20they%20cant/Sector-Automation-Key.ashx?h=557&w=720>

²⁰ Carfagna, B. Speciale TG1 del 26 ottobre 2015: <http://www.rai.it/dl/RaiTV/programmi/media/ContentItem-c0623097-0669-4734-8dae-69772ccd87a.html>. Mayer, M. (et,al.) https://www.academia.edu/14336129/International_Politics_in_the_Digital_Age, https://www.academia.edu/4509736/La_politica_Internazionale_nellEra_Digitale_bozza_da_non_citare_

²¹ Si veda: <https://teamdigitale.governo.it/en/42-content.htm>

²² Intervista Repubblica del 20 settembre 2016, p. 13: http://www.repubblica.it/economia/2016/09/30/news/digitale_diego_piacentini-148802419/