

USA-Cina. Una guerra Hi-Tech che danneggia tutti e da cui l'Europa deve sfilarsi

Alcuni giorni fa la Cina ha presentato la sua “**Global Initiative on Data Security**” (**GIDS**), un programma attraverso il quale il governo cinese intende proporre un cambio di passo sui temi di interesse internazionale legati alla sicurezza, alla tutela dei dati, al rispetto delle sovranità nazionali.

L'iniziativa, presentata dal ministro degli esteri cinese **Wang Yi**, ha avuto grande eco sulla stampa internazionale, ma è stata del tutto trascurata dai media italiani. Eppure, la proposta cinese si colloca in un contesto di relazioni internazionali tra USA e Cina, tra le due più importanti potenze economiche del pianeta, giunte ai ferri corti e ad un passo da vistose e più gravi rotture.

Come è noto il presidente **Donald Trump** ha lanciato, giusto poche settimane prima dell'iniziativa cinese **GIDS**, il piano “**Clean Network**”: un piano nel quale rientrano il blocco alle esportazioni USA verso **Huawei Technologies**, l'ordine a Paesi terzi di non vendere *micro-chips* con tecnologie americane a Huawei ed in cui rientrano anche i percorsi per mettere al bando **TikTok** e **Tencent** negli USA. Il piano Clean Network, a quanto dichiarato dal Dipartimento di Stato, avrebbe raccolto l'adesione di 30 Paesi e di numerose aziende, ma l'amministrazione americana non ha mai specificato alcunché sulle adesioni al Piano. Le ragioni addotte dagli americani sono legate alla sicurezza nazionale e alla raccolta indebita di dati di cittadini americani, accuse che le due società cinesi hanno contestato e rispedito al mittente.

Il contesto dello scontro USA-Cina è, come è noto, ben più ampio, anche se focalizzato sulle tecnologie ICT con particolari punte di intensità sui settori tecnologici del **5G** e dell'**Intelligenza Artificiale** (IA). Si tratta di due aree attigue su cui si giocherà il futuro delle economie mondiali, dal momento che **5G** e **IA** saranno alla base degli sviluppi produttivi dell'**Industria 4.0**, da cui discenderà ogni ricchezza per i prossimi decenni.

Prima di fare ulteriori considerazioni sugli elementi di contesto, vediamo più in dettaglio i termini della proposta cinese, del "**Global Initiative on Data Security**" (**GIDS**), perché gli aspetti che sollecita hanno rilevanza per tutti noi e corrispondono alle esigenze di un comune sentire degli Stati nazionali, dei gruppi di interesse e dei cittadini a livello globale.

La proposta del governo cinese fa riferimento a quattro aree che inevitabilmente si intersecano tra loro: il progresso tecnologico, lo sviluppo economico, la protezione della sicurezza nazionale e, infine, l'interesse pubblico.

L'iniziativa rilancia l'opportunità, per tutti gli Stati, di sostenere e sviluppare un contesto aperto, corretto e non discriminatorio, per consentire il vicendevole beneficio a tutti e la condivisione di ogni sviluppo derivato dall'uso di tecnologie avanzate. Allo stesso tempo, sottolinea il piano cinese, gli Stati hanno la responsabilità e il diritto di assicurare la protezione dei dati rilevanti per il Paese, dei dati personali dei loro cittadini, per la sicurezza nazionale, pubblica ed economica, assieme alla stabilità sociale.

Obiettivo dell'iniziativa?

Auspicare la convergenza di tutte le parti in commedia per la creazione di un terreno di dialogo e cooperazione sulla base del rispetto reciproco e la costruzione di un futuro condiviso nel cyberspazio, capace di portare "...pace, sicurezza,

apertura, cooperazione ed ordine", sulla base di 8 azioni operative che, secondo il governo cinese, prevedano che:

1. Gli Stati gestiscano i dati sulla sicurezza in modo completo, obiettivo, basato su evidenze, per mantenere aperta, sicura e stabile, la *supply chain* dei prodotti e dei servizi globali nell'ICT.
2. Gli Stati debbano sostenere atteggiamenti chiari contro qualunque attività che danneggi o sottragga dati importanti per le infrastrutture critiche dello Stato o usi dati nazionali per condurre attività che minino la sicurezza e l'interesse pubblico di altri Stati.
3. Gli Stati debbano prendere ogni iniziativa per prevenire o bloccare ogni attività che metta a repentaglio le informazioni personali raccolte attraverso l'ICT ed opporsi alla sorveglianza di massa di altri Stati o alla raccolta non autorizzata di informazioni personali di altri Stati attraverso strumenti di ICT.
4. Gli Stati debbano incoraggiare le società private a rispettare la legge e le norme degli Stati dove operano. Gli Stati dovrebbero evitare di chiedere ad aziende nazionali di immagazzinare e gestire dati generati e raccolti in territori diversi da quello nazionale.
5. Gli Stati debbano rispettare la sovranità, la giurisdizione e la *governance* dei dati di altri Stati e non raccogliere dati custoditi in altri Stati attraverso l'uso di aziende o individui, senza il permesso dello Stato a cui quei dati appartengono.
6. Se gli Stati hanno bisogno di ottenere dati dall'estero, per esigenze di applicazione di legge, come nel caso della lotta alla criminalità, dovrebbero farlo attraverso apposita assistenza giudiziaria o altri accordi multilaterali e bilaterali pertinenti. Qualsiasi accordo bilaterale sull'accesso ai dati tra due Stati non dovrebbe violare la sovranità giudiziaria e la sicurezza dei dati di uno Stato terzo.
7. I fornitori di prodotti e servizi ICT non dovrebbero

installare *backdoor* nei loro prodotti e servizi, per ottenere illegalmente i dati degli utenti e/o controllare o manipolare i sistemi e i dispositivi degli utenti.

8. Le aziende ICT non dovrebbero perseguire interessi illegittimi, approfittando della dipendenza degli utenti dai loro prodotti, né costringere gli utenti ad aggiornare i propri sistemi e dispositivi. I fornitori di prodotti dovrebbero impegnarsi a informare tempestivamente i loro partner di cooperazione e gli utenti di gravi vulnerabilità nei loro prodotti e offrire rimedi.

Si tratta di 8 punti cruciali per tutti, attraverso cui le autorità cinesi affermano il doppio principio del rispetto della sovranità cyber o digitale o della tutela della localizzazione dei dati. La stessa esistenza del sistema Great Firewall, che impedisce a **Google** e **Facebook** di operare in Cina, si configura come una misura estrema di difesa dei dati dei cittadini cinesi e delle infrastrutture critiche dalla pervasiva azione di due Big Tech di così grande potenza nell'accaparramento dei dati e nel controllo di ogni informazione che transiti attraverso i propri sistemi.

Il fenomeno, come si può immaginare è ben più ampio, e rischia di rientrare nel graduale processo di balcanizzazione della rete, che non si limita alla creazione di gigantesche intranet nazionali (come in Cina o in Russia o in altri Paesi che hanno già fatto questa scelta). Le circostanze dicono che la corda si sta tirando sempre più (anche a causa delle estremizzazioni necessarie a **Trump** nella sua campagna per le presidenziali di novembre), ma non è detto, come è sperabile, che debba per forza rompersi. E, anzi, auspicabile che riprendano corpo le prassi ordinarie degli organismi internazionali il cui ruolo è proprio quello di creare camere di compensazione nelle tensioni tra Stati.

Nel corso della presentazione, il ministro degli esteri cinese

Wang Yi aveva ribadito un preciso riferimento ad uno degli aspetti più critici: *"...L'appello è anche a tutte le aziende produttrici di apparati per non creare backdoors nei prodotti o servizi offerti, ovvero soluzioni nascoste attraverso le quali raccogliere indebitamente i dati personali contenuti nei flussi di informazioni trasportate, evitando qualsiasi forma di sorveglianza indebita sulle informazioni che appartengono ad altri Paesi e riguardano cittadini di altre nazioni"*.

E che i toni non siano destinati ad abbassarsi lo ha confermato il tono delle accuse agli USA, accusati da **Wang Yi** di *"bullismo poco diplomatico"*, con le decisioni unilaterali di danneggiare le imprese cinesi di Hi-Tech, anzi di danneggiare aziende *"...che esprimono livelli di competitività molto elevati"* (alterando, quindi, le ordinarie dinamiche di mercato) e con un'azione aggressiva tesa a isolare la Cina nella percezione dell'opinione pubblica dei Paesi avanzati.

Come è noto, l'amministrazione Trump ha fatto della vicenda un vessillo elettorale di peso ed ha esercitato nel corso degli ultimi mesi pressioni molto forti sia sui Paesi del cosiddetto raggruppamento **Five Eyes** (oltre a USA, ci sono Canada, UK, Australia e Nuova Zelanda), sia sui Paesi europei.

Il risultato non è stato univoco. La **Germania** ha risposto picche alle pressioni americane. Del resto il Paese è il principale partner commerciale europeo della Cina ed è di qualche giorno fa la pressione della Cancelliera **Angela Merkel**, perché la Cina apra a **Deutsche Telekom**. La **Francia**, ha adottato un atteggiamento analogo, mentre la Spagna ha per il momento chiuso le porte. Situazione *stop-and-go* in Italia, dove non sembra al momento prevalere un atteggiamento più attento agli interessi del Paese, ma si registra una certa resistenza ai diktat dell'amministrazione americana.

Il vero problema è che l'intera architettura della campagna sulla presunta volontà da parte di aziende cinesi di carpire dati di cittadini di Paesi democratici da trasferire in Cina,

per ragioni di sorveglianza globale, non ha alcun riscontro. La stessa *boutade*, presentata qualche giorno fa dal quotidiano **Il Foglio** (in Italia e all'estero da altre testate) come uno scoop senza precedenti, ovvero il caso di informazioni su personalità occidentali (tra cui alcune migliaia di italiani) raccolte in Cina, si rifaceva a informazioni anagrafiche disponibili in chiaro su internet.

In tutta questa bagarre, solo pochi ricordano che 5-6 grandi oligarchie di **Big Tech** statunitensi, raccolgono, da oltre 10 anni, miliardi di informazioni e dati personali di centinaia di milioni di persone, informazioni e dati personali in qualche caso molto dettagliati e riservati, comprese enormi quantità di informazioni sanitarie. Oggetto di tali attenzioni tutti i cittadini di tutti i paesi avanzati e non.

Montagne di informazioni e dati personali raccolti attraverso social, acquisti online, sistemi informativi aziendali, comunicazioni tra persone, tracciamenti di centinaia di milioni di telefonini.

Montagne di informazioni e dati personali che vengono spesso custoditi in sistemi Cloud trasferiti ovunque nel mondo e che quando sono custodite in sedi europee sono abbondantemente spiate e analizzate.

Montagne di dati che, se custoditi in apparati Cloud di proprietà americana, possono essere in qualunque momento soggetti a quanto previsto dal **Cloud Act**, norma americana approvata nel febbraio 2018 che consente all'amministrazione americana di avere accesso a qualunque *storage* di dati custoditi presso aziende americane in ogni parte del mondo. Naturalmente si tratta di un obbligo di aziende americane verso il governo del loro Paese, ma si tratta altresì di un obbligo che per non essere rispettato deve esser fatto mantenendo all'oscuro il cliente servito nel Paese d'origine dei dati e le stesse autorità del Paese in questione.

Montagne di informazioni che, una volta raccolte, vengono trattate da sofisticati sistemi di intelligenza artificiale capaci di creare per ciascun profilo, tra centinaia e centinaia di milioni di persone, millimetrici psico-grammi che profilano vita e miracoli di ciascuno, carattere, temperamento e tratti comportamentali.

Montagne di dati che registrano chi siete, come state, quali sono le vostre finanze, i vostri affetti, i vostri difetti e i vostri vizi, ma anche quale aspettativa di vita in base alle vostre condizioni di salute e quale previsione di comportamenti in base a ciò che abitualmente fate. Tutte informazioni che non servono assolutamente solo per orientare i vostri acquisti. Una montagna del genere non partorisce un minuscolo topolino.

<https://www.key4biz.it/usa-cina-una-guerra-hi-tech-che-danneggia-tutti-e-da-cui-leuropa-deve-sfilarsi/323446/>