

# Security Summit 2020

Sessione

## "La sovranità tecnologica e digitale dell'Unione Europea: il difficile ruolo di mediazione con gli over the top e i rapporti con gli USA"

12 novembre 2020

Intervento di

**Pasquale Stanzone**

**Presidente del Garante per la protezione dei dati personali**



**GARANTE  
PER LA PROTEZIONE  
DEI DATI PERSONALI**

Tra le tante contraddizioni del nostro tempo viene in evidenza una che, forse più di altre, sembra destinata a perdurare ancora a lungo, vantando anche radici antiche. E' il paradosso del riemergere, quasi carsico, di miopi sovranismi e nazionalismi, a fronte di una crisi profonda della sovranità e dei suoi attributi paradigmatici: dal controllo del territorio- i cui confini si relativizzano nel contesto dematerializzato della realtà virtuale - al monopolio dello *jus dicere*, progressivamente eroso dalle innumerevoli "giurisdizioni private" (board, adr e così via), promosse sempre più in materia consumeristica e non solo. Tra le scaturigini di questa contraddizione vi è, in posizione tutt'altro che secondaria, la rivoluzione digitale, con le sue implicazioni e la sua antropologia, che hanno rivoluzionato le coordinate essenziali su cui sinora si sono fondati sistemi istituzionali, relazioni sociali, il sostrato culturale e persino simbolico del nostro vivere.

Interrogarsi sull'idea di sovranità digitale in un'epoca, come l'attuale, di ripensamento radicale del senso e degli attributi della sovranità - insidiata da sempre più pervasivi poteri privati - vuol dire allora analizzare i punti nodali della nostra società e coglierne fino in fondo l'evoluzione. Nessuna "microfisica" del potere, per riprendere Michel Foucault, potrebbe oggi prescindere dall'analisi dell'impatto dirompente del digitale sul nostro vivere, in privato e in pubblico, e sulla stessa dinamica democratica.

Della sovranità digitale si possono dare varie letture. Viene proposta una minimalista, forse anche più materiale e pragmatica, che enfatizza l'esigenza di indipendenza nazionale nella fornitura, gestione e finanche negli stessi assetti proprietari delle infrastrutture tecnologiche. È il tema che ricorre spesso a fronte dei casi di acquisizione, da parte di aziende straniere, del controllo societario rispetto ad asset strategici, quali ad esempio le telecomunicazioni.

Ed è l'idea sottesa alla frequente proposta di un cloud europeo (e via via scendendo di livello, nazionale), inteso come disponibilità esclusiva, da parte di ciascun Paese o area (come per l'UE) di proprie infrastrutture tecnologiche che consentano di spezzare

quella dipendenza- non solo funzionale - da fornitori stranieri (generalmente cinesi o americani), della cui opportunità sempre più si dubita.

Questa declinazione "materialistica" della sovranità nazionale coglie, senza dubbio, la rilevanza del rapporto tra l'assetto dominicale delle tecnologie e la loro funzionalità anche in termini democratici, sottolineando l'esigenza di una governance non soltanto interna (non straniera) ma, soprattutto, pubblica delle principali infrastrutture digitali.

La delega, a terzi, della gestione degli snodi essenziali attraverso cui transitano informazioni strategiche per il Paese evidenzia, poi, la rilevanza (non solo sociale, ma financo giuridica e politica) progressivamente assunta da sempre più forti poteri privati (gli OTT in particolare), in quella che progressivamente si configura come società delle piattaforme. Esse, infatti, sono oligopoliste non tanto e non soltanto in ragione della loro potenza economica e commerciale, quanto piuttosto per il possesso della principale infrastruttura sociale, oltre che tecnologica: la rete. Tale possesso garantisce loro un potere di condizionamento che nessun mezzo di comunicazione di massa poteva vantare in precedenza, perché privo di quella capacità, propria invece delle piattaforme, di orientare l'opinione pubblica agendo con la formidabile leva del *microtargeting* e della profilazione, così da segmentare l'offerta e proporre non solo pubblicità ma persino informazione mirata e, quindi, più persuasiva.

Questa capacità di condizionamento (*nudging*), propria, in tali termini, soltanto del capitalismo della sorveglianza, può avere effetti determinanti non soltanto sulle scelte individuali ma anche su quelle collettive e, persino, politico-elettorali. Come ha dimostrato il caso *Cambridge Analytica*, infatti, con il pedinamento digitale si modella il messaggio politico da promuovere, orientando il consenso elettorale verso il risultato voluto. Si eludono così le garanzie previste da decenni per il pluralismo informativo e politico, come pure per l'autodeterminazione individuale, con il rischio di una manipolazione del consenso, tale da alterare in radice i più rilevanti processi democratici. Ne viene pregiudicata persino l'altrimenti intangibile sovranità statale, ogniquale volta la manipolazione del consenso sia organizzata – come parrebbe nel caso americano – da Governi stranieri, così da orientare il risultato elettorale verso la soluzione a loro più favorevole.

E', questo, solo un aspetto dell'assunzione, da parte delle grandi piattaforme, di alcune prerogative tipiche della sovranità: il controllo della principale infrastruttura sociale, la disciplina, con le loro condizioni generali di contratto, dei modi di esercizio delle libertà, persino lo *jus dicere* tramite giurisdizioni private, divenute arbitri del rapporto tra diritti fondamentali, come avviene per oblio, discorsi ostili e via enumerando.

In questo contesto, persino la più pragmatica delle accezioni di sovranità digitale non può prescindere dall'esigenza di una governance pubblica delle infrastrutture tecnologiche che riconduca i "poteri privati" all'interno delle coordinate e della dinamica democratiche, a partire dalla riserva della decisione, in ultima istanza, sui diritti fondamentali all'autorità pubblica, secondo il modello che la privacy dati ha offerto sul terreno dell'oblio o del *cyberbullismo*.

Ma, accanto a questa, vi è una diversa accezione di sovranità digitale, declinata in chiave valoriale, alludendo cioè a quella disciplina del rapporto tra diritto, persona e tecnica che finisce sempre più per definire il profilo identitario di un ordinamento, sotto il profilo sociale, culturale, giuridico, persino politico. In questo senso, sovranità digitale vuol dire governo della tecnica secondo la gerarchia assiologica espressa da ciascun ordinamento, conformemente alla sua identità e tradizione costituzionale. E' significativo

che l'UE abbia ritrovato, in particolare sul terreno del governo antropocentrico della tecnica, un'unità smarrita da tempo in molti altri settori, riaffermando la propria identità come ordinamento fondato su alcuni, irrinunciabili, valori, non negoziabili neppure per esigenze giusinternazionalistiche (Corte di giustizia europea, sent. Kadi, pur in ambito non digitale) e, tantomeno, per ragioni di scambi commerciali con ordinamenti ispirati a un ben diverso bilanciamento d'interessi (sentenze Schrems).

Nel raffronto con gli Usa sul terreno della disciplina privacy è emersa con chiarezza quest'accezione identitaria della sovranità digitale: la Corte di giustizia europea ha, soprattutto in questi casi, contribuito a delineare l'Ue come "comunità di diritto" caratterizzata da un sistema di tutela della persona (anche e soprattutto rispetto alle insidie poste dalle nuove tecnologie) non derogabile, nel suo nucleo essenziale, neppure per quelle superiori esigenze di sicurezza nazionale che negli Usa legittimano così significative limitazioni delle libertà individuali.

Nelle due sentenze Schrems del 2015 e del luglio scorso, la Corte sottende un'idea di sovranità digitale come non subalternità del sistema europeo di tutela (anche e soprattutto) della privacy rispetto ad ordinamenti, quali quelli americani, meno garantisti e capaci dunque di neutralizzare le tutele accordate dal diritto europeo ogniquale volta i dati, nella loro inevitabile mobilità transnazionale, siano trasferiti negli Usa. Non è un caso che questa nozione valoriale di sovranità digitale, come rivendicazione di un sistema di tutele rispetto all'incidenza di altri e meno garantisti ordinamenti, sia emersa proprio sul terreno della protezione dati. Mai come rispetto a quest'ambito, infatti, le reciproche influenze ed interferenze tra ordinamenti diversi condizionano rapporti commerciali, sociali, politici, attraverso le scelte sulle tecniche di tutela dei dati personali, ad un tempo oggetto di un diritto fondamentale ma anche risorsa economica sempre più ambita, da un capo all'altro dell'Oceano.

Ecco, quindi, che riaffermare, da parte della Corte di giustizia europea, la validità delle garanzie accordate dall'ordinamento europeo e difenderle dall'erosione determinata dall'applicazione, ai dati trasferiti oltreoceano, di discipline fondate sulla preminenza di ragioni commerciali o, per altro verso, di sicurezza nazionale sui diritti della persona, ha significato per l'Europa resistere all'ibridazione con un sistema di valori incompatibili con il proprio, delineando così la propria identità in termini personalistici e garantisti.

Analogo significato ha avuto la disciplina dell'ambito territoriale di applicazione della disciplina di protezione dati che, a partire dalla sentenza Costeja del 2014, sino al Regolamento europeo, ha sostituito il criterio meramente spaziale con quello, mutuato dalla disciplina consumeristica, del "targeting", ovvero della direzione dell'offerta di beni e servizi a quanti si trovino nell'Ue. La scelta di radicare la disciplina europea anche rispetto ai titolari con sede non europea, per il sol fatto di trattare dati di quanti si "trovino" in Europa, rappresenta in questo senso un'affermazione di sovranità digitale nettissima

Infatti, questa extraterritorialità temperata della disciplina europea consente non soltanto di attrarre a sé i titani del web, assicurando a chiunque si trovi in Europa (non solo ai "cittadini", come doveroso per un diritto fondamentale) un paniere di diritti non derogabile in ragione della localizzazione della sede aziendale, superando così ogni scelta elusiva di forum shopping; ma soprattutto, questa regola diviene rappresentazione plastica di quel principio di effettività delle tutele della persona che costituisce il baricentro dell'ordinamento europeo.

La sentenza Schrems di luglio 2020 è, in tal senso, chiarissima. Nell'escludere che il *Privacy Shield* garantisca una tutela effettiva della privacy perché non azionabile dinanzi a un organo giurisdizionale realmente terzo e imparziale e nell'onerare i *data exporter* del compito di vagliare il grado di tutele accordato ai dati trasferiti negli Usa, vi è molto di più della mera responsabilizzazione dei protagonisti del trattamento e persino di più dell'esigenza di garantire agli Europei un livello di tutela 'sostanzialmente equivalente' a quello del vecchio continente anche al di fuori dei suoi confini.

Quest'ultima pronuncia sottende l'idea che il diritto alla protezione dati necessiti di una tutela "oggettiva", inesauribile nella fase negoziale, inter partes e necessitante tutele pubblicistiche effettive. La privacy, paradossalmente, appare sempre meno una mera questione "privata" e, sempre più, un tema di straordinaria rilevanza pubblica, su cui si misura la tenuta della democrazia e la stessa connotazione identitaria, assiologica, degli ordinamenti.

In questo senso, dunque, l'affermazione della sovranità digitale europea, ben lungi da pretese egemoniche o autarchiche, è invece – come ha asserito la presidente Ursula Von Der Leyen - rivendicazione di un sistema di tutele che connota l'Unione come spazio di libertà e di diritti, capace di assicurare un governo antropocentrico e personalista dell'innovazione.