COVID-19, regolazione e nuove tecnologie: vecchi problemi e nuovi tentativi di soluzione

di Sveva Del Gatto[1]

23 giugno 2020

Premessa

Lo scoppio della pandemia ha reso ancor più evidente la centralità delle nuove tecnologie per la resilienza economica e sociale di un Paese: dalle imprese, per cui è apparso chiaro come la digitalizzazione rappresenti ormai, il crocevia dove si decide chi sopravvive e chi no; ai servizi, da quelli pubblici a quelli bancari o assicurativi, che hanno, nella gran parte dei casi, potuto continuare a funzionare. Dal lavoro alla scuola, la cui continuità è stata possibile (seppur con numerose falle per quanto riguarda il sistema scolastico) grazie ad Internet e alle tante app per videoconferenze e videolezioni. La digitalizzazione e le nuove tecnologie non solo hanno permesso di evitare che la quotidianità, durante i periodi di *lockdown*, perdesse ogni tipo di normalità, ma hanno anche consentito nuovi e, prima del COVID-19, inimmaginati, sviluppi, densi di benefici per i cittadini e le amministrazioni (dalle app per la prevenzione e la lotta contro il COVID, ai servizi digitali per aiutare i bisognosi; dai sistemi di intelligenza artificiale a supporto della polizia municipale per il distanziamento sociale in spazi aperti, a quelli per il trasporto pubblico o per il calcolo in tempo reale delle distanze interpersonali e del livello dinamico del rischio di contagio in luoghi pubblici e di lavoro).

Sull'importanza di investire nell'IA, soprattutto dopo l'avvento del nuovo Coronavirus, vi è accordo unanime anche tra le istituzioni, sia a livello nazionale, sia sovranazionale e globale.

[1] Professore associato di diritto amministrativo (Università di Roma Tre).

Secondo il nuovo documento programmatico "COVID-19: Embracing digital government during the pandemic and beyond" del Dipartimento degli Affari Economici e Sociali dell'ONU (UN/DESA), occorre che i governi facciano pieno uso delle tecnologie digitali per contrastare la pandemia e affrontare l'ampia gamma di questioni ad essa connesse. In questo senso, si è pronunciata anche la Vicepresidente esecutiva della Commissione UE che, dopo aver osservato che «[l]a crisi COVID-19 ha dimostrato quanto sia fondamentale che i cittadini e le imprese siano collegati e in grado di interagire tra loro *online*», ha assicurato che l'Unione europea continuerà a «collaborare con gli Stati membri per individuare gli ambiti che necessitano di maggiori investimenti affinché tutti gli europei possano beneficiare dei servizi e delle innovazioni digitali».

L'uso delle nuove tecnologie, anche nell'era del COVID, non è tuttavia, esente da problemi e rischi che anzi, in alcuni casi, sono apparsi acuiti dalla pandemia ancora in corso.

Le questioni giuridiche che si pongono sono numerose. Le principali, su cui ci si soffermerà in queste brevi riflessioni, riguardano la tutela della *privacy* e dei diritti fondamentali dei cittadini; la necessità di una regolazione sull'uso delle nuove tecnologie, in particolare, da parte delle pubbliche amministrazioni; il rapporto tra uso delle nuove tecnologie (nella specie delle piattaforme social) e trasparenza e veridicità delle informazioni (fenomeno delle *fake-news*).

COVID-19, nuove tecnologie e tutela della privacy e dei diritti fondamentali degli individui

Il tema è strettamente legato alle app di tracciamento dei contatti, ma non si esaurisce con esse.

In merito alle app di *contact tracing,* utili nel prevenire nuovi focolai, le necessarie garanzie per la *privacy* degli utenti dipendono dalle modalità di raccolta e dalle finalità del trattamento dei dati, dal tipo di dati raccolti, dal carattere volontario o meno della App e dalla politica seguita in merito agli obblighi di distruzione dei dati imposti al gestore e alla piattaforma. Con riferimento alla gran parte di questi parametri, il Massachusetts Institute of Technology di Boston (MIT), attraverso uno studio *in progress* delle app esistenti a livello mondiale, ha evidenziato numerose lacune in termini di trasparenza, riservatezza e utilizzo dei dati (la App cinese, ad esempio, difetta su tutti i punti analizzati dal MIT, dalla mancanza di volontarietà, alla ridotta trasparenza, ed è seguita, in termini negativi, da Bulgaria, Irlanda e Malesia).

Per evitare i rischi per la *privacy* dei cittadini che questi strumenti di prevenzione possono presentare, il 1° giugno 2020, negli Stati Uniti è stato presentato l'Exposure Notification Privacy Act (ENPA), un disegno di legge bipartisan (a firma dei senatori e senatrici M. Cantwell, B. Cassidy e A. Klobuchar) che introduce una serie di obblighi e divieti per i gestori delle app di *contact tracing*.

Le principali novità della proposta (che non ha ad oggetto solo il COVID-19, ma si estende ad altre malattie infettive) sono il necessario coinvolgimento delle autorità sanitarie pubbliche e, in materia di *enforcement,* l'attribuzione della competenza a verificare l'attuazione delle norme ad un'agenzia governativa, la *Federal Trade Commission,* a cui sono assegnati specifici poteri

sanzionatori in caso di violazione dell'ENPA. La disciplina prevede inoltre, l'obbligo del consenso espresso, il divieto di utilizzare i dati per fini commerciali e l'obbligo di distruggerli entro trenta giorni.

Problemi di tutela dei diritti fondamentali sono sorti anche con riferimento all'utilizzo di *software* di riconoscimento facciale da parte delle amministrazioni, in particolare, da parte delle forze di polizia.

Già prima dell'emergenza COVID-19, l'uso di questa tecnologia aveva suscitato dubbi e proteste per l'acquisizione di dati sensibili senza il consenso degli interessati, per il coinvolgimento delle società private nell'elaborazione dei *software* di AI, per l'esistenza di ampi margini di errore alimentati dalla scarsa qualità delle immagini acquisite e per il rischio di discriminazioni legate al genere o alla razza (si veda, al riguardo il Rapporto 2019 della FRA - Agenzia europea per i diritti fondamentali). In Galles, ad esempio, l'utilizzo di tecniche di riconoscimento facciale è stato oggetto di un ricorso da parte di alcune associazioni a tutela dei diritti fondamentali, poi conclusosi però, con una sentenza che ne ha riconosciuto la legittimità ai sensi dell'art. 8 CEDU e del GDPR. Negli Stati Uniti, dove l'uso del riconoscimento facciale da parte delle forze dell'ordine e delle agenzie governative è frequente ma avviene, spesso, in assenza di specifica regolazione, l'ACLU (*American Civil Liberties Union*) ha recentemente presentato un ricorso contro *Clearview* una società privata che figura tra i principali fornitori di *software* di *facial recognition* del governo americano.

Il COVID-19 ha accentuato le questioni giuridiche sopra richiamate, per due ordini di ragioni. In primo luogo, perché è stato incrementato l'uso di tecniche di riconoscimento facciale da parte delle agenzie governative per finalità di interesse generale, utilizzandole, ad esempio, per verificare, insieme ad altri strumenti, come i *termoscanner*, lo stato di salute di un soggetto e farne discendere la possibilità o meno di fruire di determinati servizi. In secondo luogo, perché l'uso diffuso della mascherina ha aumentato il margine di errore, nonostante siano già stati realizzati e sperimentati *software* che consentirebbero il riconoscimento anche con il viso parzialmente coperto.

La necessità di regole e garanzie nei confronti dell'uso delle nuove tecnologie da parte delle amministrazioni

Un secondo ordine di problemi, emerso già da quanto sopra, riguarda la necessità di introdurre regole che disciplinino espressamente l'uso delle nuove tecnologie, in particolare da parte delle amministrazioni pubbliche e che prevedano idonee garanzie, anche procedimentali, nei confronti dei cittadini/utenti.

La questione è emersa sia nell'Unione europea, sia negli Stati Uniti, ma le soluzioni seguite sono state sostanzialmente diverse.

Nell'Unione europea, le norme della CEDU e quelle GDPR, seppur non specifiche per le singole tecnologie (riconoscimento facciale, app di tracciamento, ecc.), sono state considerate adeguate a risolvere le relative questioni giuridiche sorte in merito al rispetto dei diritti degli interessati.

L'esistenza di regole e principi comuni ha, dunque, avuto in Europa, un duplice effetto: ha impedito che eventuali nuove normative sull'IA adottate a livello nazionale generassero difformità regolatorie tra gli Stati membri e ha consentito di evitare, in assenza di una regolazione nazionale *ad hoc*, un vuoto di regolazione.

Al riguardo, di particolare interesse risultano due vicende giurisprudenziali recenti. In un caso, già sopra richiamato, volto a sindacare la legittimità dell'uso della tecnologia di *facial recognition* da parte della polizia del Galles, la Corte di giustizia di Cardiff ha ritenuto legittimo il riconoscimento facciale in quanto proporzionato e rispettoso dei criteri stabiliti dall'articolo 8, paragrafo 1, CEDU (in particolare, le tecniche usate hanno superato il c.d. *Bank Mellat test*).

Nel secondo caso, invece, la Corte distrettuale dell'Aia ha censurato l'operato del Ministero delle politiche sociali olandese che aveva utilizzato un algoritmo per valutare l'attitudine di una parte più svantaggiata della popolazione a commettere frodi per l'ottenimento di sussidi pubblici. Secondo i giudici, l'azione dell'amministrazione, pur legittima ai sensi del già citato art. 8, è avvenuta in violazione dell'art. 7 del GDPR, in quanto priva di garanzie procedimentali, opaca, scarsamente *accountable* e poiché le decisioni prese sono risultate eccessivamente influenzate dai privati proprietari del *software* usato.

L'esistenza di una normativa comune a livello sopranazionale che opera anche in assenza di indicazioni specifiche dei singoli Stati, appare quanto mai cruciale nell'attuale fase pandemica. La previsione espressa di garanzie, infatti, accresce la "fiducia", spesso scarsa (come segnalato nel Libro Bianco della Commissione UE sull'intelligenza artificiale) del cittadino/utente che di conseguenza è più stimolato all'utilizzo della tecnologia. Ciò, come dimostra il caso delle app di *contact tracing,* ha effetti diretti sulla effettività dei benefici legati a tali sistemi in termini di tutela della salute pubblica e di prevenzione.

Diverso è, invece, l'esempio degli Stati Uniti dove manca una disciplina comune di carattere generale e ogni Stato può autonomamente scegliere di vietare o consentire l'uso di nuove tecnologie e come disciplinarle (si pensi al riconoscimento facciale permesso ed espressamente disciplinato a Washington, espressamente vietato dalla Città di San Francisco, consentito ma non espressamente disciplinato in altri Stati).

L'approccio settoriale e i limiti ad esso legati potrebbero essere in parte superati, per quanto riguarda le app di tracciamento dei contagi, nel caso in cui fosse approvata l'ENPA, la proposta di legge federale già sopra richiamata, a tutela della *privacy* degli utenti. I contenuti della proposta, in larga misura condivisibili, appaiono però, in vari punti significativamente influenzati da colossi della tecnologia come Apple e Google. L'influenza dei *Big Tech* nella stesura di disegni di legge relativi alle tecnologie digitali non va in sé respinta. Essa è, infatti, da una parte inevitabile, per un necessario intreccio tra tecnica e politica, e dall'altra, potenzialmente foriera di effetti positivi (la politica dei *Tech Giants* sulla *privacy* e sulla sicurezza dei dati è molto stringente e può essere, come accaduto nel caso dell'ENPA, presa a modello). Vi è tuttavia, il rischio, non sempre solo potenziale, di riconoscere ai grandi operatori privati della tecnologia un ruolo eccessivo nelle decisioni sul contenuto di norme volte a tutelare i diritti dei cittadini proprio da un uso distorto delle nuove tecnologie. Va quindi, garantito che sull'individuazione del giusto equilibrio tra la tutela della *privacy* e la protezione della salute pubblica (o di altri diritti fondamentali) non pesino considerazioni di *marketing*.

COVID-19, nuove tecnologie e *fake-news*

L'ultimo punto riguarda, infine, il tema dei rischi di scarsa trasparenza nelle informazioni rinvenute su internet e in generale, sui *social media* e delle conseguenze negative legate alle *fake news* che la pandemia ha contribuito ad evidenziare (si pensi che durante il *lockdown* il numero delle persone che si sono affidate ad internet per informazioni e consigli legati al COVID-19 è aumentato esponenzialmente).

La risposta del governo italiano, ma non solo, è stata nel complesso positiva. Secondo il documento programmatico dell'UN/DESA già citato, una revisione dei portali nazionali degli Stati membri delle Nazioni Unite ha riscontrato un notevole aumento di informazioni e indicazioni sul nuovo Coronavirus rese disponibili già agli inizi di aprile.

L'importanza di assicurare un'informazione trasparente e veritiera è stata sottolineata dall'Unione europea che il 10 giugno ha pubblicato la comunicazione congiunta "Tackling COVID-19 disinformation - Getting the facts right" (JOIN(2020) 8 final) in cui già nelle prime righe si osserva che «[t]he COVID-19 ('Coronavirus') pandemic has been accompanied by an unprecedented 'infodemic'. A flood of information about the virus, often false or inaccurate and spread quickly over social media, can – according to the World Health Organisation (WHO) – create confusion and distrust and undermine an effective public health response».

Analogamente, a livello nazionale, è stata istituita nell'aprile scorso, presso il Dipartimento per l'informazione e l'editoria, l'Unità di monitoraggio per il contrasto della diffusione di *fake news* relative al COVID-19 sul *web* e sui *social network* che di recente ha pubblicato alcune proposte e linee guida sul tema.

Da un punto di vista giuridico, le questioni principali che qui si pongono riguardano la responsabilità delle piattaforme, l'individuazione di specifici obblighi di trasparenza a cui le stesse dovrebbero sottostare e la legittimità di comportamenti di rimozione di determinati contenuti da parte della piattaforma. Si pensi, al riguardo, alla recente vicenda che ha coinvolto Twitter e il Presidente Trump e in precedenza, in Italia, all'oscuramento della pagina FB di Casapound e di Forza Nuova. In questo caso, fanno riflettere i pronunciamenti di segno opposto intervenuti sul tema. La sezione specializzata in materia di impresa del Tribunale civile di Roma (ordinanza del 12 dicembre 2019) ha accolto il ricorso di CasaPound censurando l'operato di Facebook, per violazione del principio del pluralismo dei partiti politici (49 Cost.).

Al contrario, la sezione diritti della persona e immigrazione civile sempre del Tribunale civile di Roma (ordinanza del 23 febbraio 2020) ha confermato la legittimità dell'oscuramento da parte di Facebook della pagina di Forza Nuova, osservando che tra i limiti alla libertà di manifestazione del pensiero, nel bilanciamento con altri diritti fondamentali della persona, deve assumere un particolare rilievo il rispetto della dignità umana ed il divieto di ogni discriminazione, a garanzia dei diritti inviolabili spettanti ad ogni persona.

Al fine di risolvere tali questioni e le altre sopra indicate, sarebbe quindi opportuna, se non necessaria, l'approvazione nel nostro ordinamento di una regolazione *ad hoc* che bilanciasse la libertà di informazione e pluralismo con i principi di trasparenza, *privacy* e *due process of law*.