TECNICA, PROTEZIONE DEI DATI E NUOVE VULNERABILITÀ*

Pasquale Stanzione**

1. Il capitalismo delle piattaforme.

La permanenza della condizione pandemica ci ha insegnato a convivere con le limitazioni dei diritti, tracciando tuttavia il confine che separa la deroga dall'anomia, dimostrando come la democrazia debba saper lottare, sempre, con una mano dietro la schiena.

Ma quella della democrazia liberale contro le derive autoritarie è una vittoria da rinnovare giorno per giorno mai dandola per acquisita, come ha fatto l'Europa che ha dimostrato, anche in quest'occasione, di saper coniugare, senza contrapporle, libertà e solidarietà, sfuggendo alla tentazione delle scorciatoie tecnocratiche della biosorveglianza.

E se la traslazione *on line* della vita e la funzionalizzazione, a fini sanitari, della tecnica è stata possibile senza cedere allo stato di eccezione, ciò non ha comunque potuto impedire una profonda trasformazione sociale, culturale e perfino antropologica di cui la pandemia è stata un catalizzatore, rivelando quanto sia profonda l'interrelazione tra la nostra vita e il digitale.

A partire dai primi mesi di *lockdown* e con effetti, tuttavia, verosimilmente destinati a perdurare, alle piattaforme è stata affidata la stragrande maggioranza delle nostre attività quotidiane; la parte più significativa degli scambi commerciali è avvenuta *on-line*, persino le prestazioni sociali più rilevanti (dalla scuola all'università, dai servizi amministrativi alla giustizia) sono state erogate da remoto.

In fondo, se il distanziamento fisico imposto per esigenze sanitarie non è divenuto anche sociale, lo si deve alle nuove tecnologie, capaci di ricreare nello spazio virtuale quei legami impediti nel reale, pur costringendoci a ripensare il sistema delle garanzie nel passaggio dall'*off-line* all'*on-line*. La stessa "scommessa" del green pass – quale misura di prevenzione sanitaria necessaria per far ripartire il Paese – si fonda sulla capacità dei sistemi informativi di fornire una rappresentazione aggiornata della condizione di ciascun soggetto e, come il Garante ha tenuto a ribadire, sull'utilizzo dei soli dati strettamente indispensabili a dimostrarla.

* Intervento alla giornata di studi "La tutela della *privacy* durante l'emergenza Covid 19" del 19 ottobre 2021, ore 10.30, presso l'aula Magna "Vincenzo Buonocore" dell'Università degli Studi di Salerno.

** Professore emerito di Diritto privato dell'Università degli Studi di Salerno. Presidente Autorità garante per la protezione dei dati personali.

Il digitale ha, così, dimostrato di poter essere al servizio dell'uomo, ma non senza un prezzo di cui bisogna avere consapevolezza: l'accentramento progressivo, in capo alle piattaforme, di un potere che non è più soltanto economico, ma anche - e sempre più - performativo, sociale, persino decisionale.

Un potere che si innerva nelle strutture economico-sociali, fino a permeare quel "caporalato digitale" rispetto ai lavoratori della *gig economy,* protagonisti (anche in Italia) del primo sciopero contro l'algoritmo: gli "invisibili digitali", come da taluno sono stati definiti.

I "gatekeepers", appunto, stanno assumendo un ruolo sempre più determinante nelle dinamiche collettive, economiche, persino politiche, assurgendo a veri e propri poteri privati scevri, tuttavia, di un adeguato statuto di responsabilità**.**

La pandemia ha dimostrato l'indispensabilità dei servizi da loro forniti ma, al contempo, anche l'esigenza di una strategia difensiva rispetto al loro pervasivo 'pedinamento digitale'**,** alla supremazia contrattuale, alla stessa egemonia "sovrastrutturale", dunque culturale e informativa, realizzata con pubblicità mirata e *microtargeting.*

Di più. La sospensione degli account Facebook e Twitter di Donald Trump ha rappresentato plasticamente come le scelte di un soggetto privato, *quale il gestore di un social network,* possano decidere le sorti del dibattito pubblico, limitando a propria discrezione il perimetro delle esternazioni persino di un Capo di Stato.

E nel nostro ordinamento, a fronte dell'oscuramento del profilo *social* di un movimento politico per diffusione di contenuti contrari alla *policy* del gestore, il Tribunale di Roma ha rilevato come il pur ordinario contratto privatistico di fornitura del servizio di *social network* soggiaccia a una peculiare forma di eteroregolazione dovuta alla sua incidenza su diritti fondamentali.

E' questo il nodo di fondo del capitalismo delle piattaforme: l'esigenza di una loro cooperazione nell'impedire che la rete divenga uno spazio anomico dove impunemente si possano violare diritti, senza tuttavia ascrivere loro un ruolo arbitrale rispetto alle libertà fondamentali e al loro bilanciamento, da riservare pur sempre all'autorità pubbli*ca.*

Su questo crinale stretto si muove il *Digital Services Act,* così da introdurre forme di responsabilizzazione delle piattaforme, il cui potere di moderazione dei contenuti viene assoggettato ad obblighi di trasparenza e a rimedi impugnatori che ne consentano un sia pur minimo sindacato esterno.

Non è un caso che, negli Usa, l'accesso alla "scatola nera" degli algoritmi, per verificarne l'impatto sulla circolazione delle notizie, sulla loro amplificazione e dunque sulla formazione

dell'opinione pubblica, sia divenuto oggetto di richieste sempre più frequenti da parte di esponenti politici di opposti schieramenti.

Questa potentissima forma di "*nudging*", tesa ad orientare le scelte degli utenti secondo la stima predittiva dell'algoritmo, rivela quanto i singoli siano disarmati di fronte al potere performativo del digitale.

In un contesto definito di "capitalismo estrattivo"- per l'attitudine predatoria delle piattaforme nei confronti dei dati, liberamente attinti come fossero res nullius - è indispensabile rafforzare – come ha fatto ad esempio la Corte di giustizia europea con la sentenza di novembre sul consenso on line e come fa lo schema di regolamento e-privacy - l'autodeterminazione informativa.

L'autodeterminazione informativa è, infatti, il necessario presupposto di scelte libere e, appunto, consapevoli, in un contesto in cui servizi apparentemente gratuiti sono invece pagati al caro prezzo dei nostri dati e, quindi, della nostra libertà. Perché "quando è gratis, il prodotto sei tu".

2. La "geopolitica" della privacy.

Una più netta presa di coscienza del valore dei propri dati è l'unico, effettivo baluardo contro il rischio della monetizzazione della privacy, che rappresenta oggi la vera questione democratica nel governo della rete.

Da un lato, infatti, la *zero price economy* ha reso prassi ordinaria lo schema negoziale 'servizi contro dati'; dall'altro, riconoscere la possibilità della remunerazione del consenso rischia di determinare una rifeudalizzazione dei rapporti sociali, ammettendo che si possa pagare con i propri dati e, quindi, con la propria libertà.

Su questo "pendio scivoloso" è in gioco, forse più che in ogni altro campo, l'identità europea come "Comunità di diritto", fondata sulla sinergia tra libertà, dignità, eguaglianza, quali presidi essenziali che nessuna ragion di Stato o, tantomeno, di mercato può violare.

E' significativo che l'Unione Europea abbia negli ultimi cinque anni (a partire, in particolare, dal nuovo quadro giuridico sulla privacy, sino alla recente *Bozza* sull'intelligenza artificiale) messo al centro della propria agenda politica la regolazione del digitale, consapevole che l'anomia cui altrimenti sarebbe consegnata la rete non esprime libertà, ma soggezione alla *lex mercatoria*, tanto quanto alla *lex informatica*.

Se "code is law" è perché il digitale esprime un nuovo paradigma di senso, un nuovo ordine antropologico e simbolico che va coniugato con il sistema, anzitutto di valori, proprio del *rule of law* cui s'ispira la costruzione europea.

E proprio sul governo antropocentrico del digitale l'Unione europea sta promuovendo - adesso anche con la *Bozza* di regolamento citata - uno sviluppo sostenibile dell'innovazione, che la renda funzionale al progresso sociale.

Questa vocazione personalista contraddistingue, certamente, le politiche dell'innovazione europee dall' "imperialismo digitale" cinese, con la sua pericolosa alleanza tra potenza di calcolo e potere coercitivo, di cui il *social credit system* e il riconoscimento facciale (persino "emotivo") sono un esempio emblematico.

Ma la "differenza" europea connota, ancora una volta sul terreno della privacy, anche il rapporto con gli Stati Uniti, sia per l'approccio liberistico all'innovazione, sia per il rapporto tra garanzie individuali e sicurezza nazionale.

Con la sentenza *Schrems* II del luglio 2020, infatti, la Corte di giustizia europea ha invalidato anche il *Privacy Shield* e la conseguente decisione di adeguatezza dell'ordinamento americano in ragione della carenza, per i dati lì trasferiti, di garanzie sostanzialmente equivalenti a quelle sancite dalla disciplina dell'Unione.

Ciò dimostra come la privacy necessiti di una tutela "oggettiva", che non si esaurisce nella fase negoziale rimessa alla sola disponibilità delle parti, ma esige tutele pubblicistiche effettive.

La privacy, come è stato detto, appare paradossalmente sempre meno una mera questione "privata" e, sempre più, un tema di rilievo pubblico centrale, su cui si misura, anche in termini geopolitici, la tenuta dello Stato di diritto.

Nella valutazione di (in)adeguatezza del sistema di tutele accordate dall'ordinamento americano ha avuto un peso determinante il regime di accesso ai dati per fini investigativi, modulato in forme assai diverse da quelle invalse in Europa e ritenute determinanti ai fini della "identità costituzionale" europea.

La Corte di giustizia, sotto questo profilo, ha valorizzato la funzione democratica della privacy, capace di realizzare l'equilibrio tra libertà e sicurezza prescritto dall'art. 6 della Carta di Nizza e valorizzato ulteriormente da una recente pronuncia CEDU sull'illegittimità della sorveglianza massiva.

Il terreno elettivo di questa lettura garantista è stato, sin dalla sentenza *Digital Rights*, quello della *data retention*, rispetto alla quale proprio nei mesi scorsi la Corte ha sancito alcune affermazioni importanti.

*C*on la sentenza del 2 marzo la Corte ha chiarito come l'acquisizione dei tabulati esiga il vaglio di un'autorità effettivamente terza rispetto all'organo inquirente e vada limitata ad esigenze di contrasto di gravi reati o minacce per la sicurezza pubblica.

Tali esigenze di garanzia sono state così valorizzate, su indicazione anche del Garante, dal legislatore nazionale, pur con l'esigenza che tuttora permane di revisione della disciplina della durata della conservazione dei tabulati, nel segno del canone di proporizonalità.

3. Nuove vulnerabilità.

In un contesto così complesso come l'attuale, caratterizzato dalla convergenza tra potenza di calcolo ed emergenza, suscettibile di alterare il sistema delle garanzie democratiche, la disciplina della privacy, nell'applicazione quotidiana dell'Autorità, si è rivelata uno strumento prezioso.

Nell'affrontare queste sfide il Garante ha assunto, quale obiettivo prioritario, la tutela della persona rispetto alle nuove vulnerabilità ingenerate dall'accelerazione esponenziale del processo di transizione digitale.

Ciò è emerso univocamente sul terreno della tutela della persona *on-line*, rispetto ai rischi di coinvolgimento dei minori in situazioni per loro inadeguate e, quindi, pericolose o riguardo all'uso, a fini ritorsivi o altrimenti pregiudizievoli, dell'immagine altrui.

Con il provvedimento nei confronti di Tik Tok il Garante ha inteso esigere il rispetto degli obblighi imposti dal Regolamento europeo a tutela del minore *on line*: prima fra tutte, la verifica dell'età dell'utente, che, al di sotto della soglia minima di età prevista, non può fruire dei social.

Naturalmente, l*'age verification* è una condizione necessaria, ma non sufficiente per rendere il *web* un ambiente se non sicuro, almeno non inospitale per i minori.

Per raggiungere quest'obiettivo si deve promuovere una reale pedagogia digitale e rendere effettiva la responsabilità per i contenuti illeciti diffusi.

Del resto, ogni dato "abbandonato" in rete è un dato perso, affidato alle scelte, non sempre responsabili e leali, che altri faranno (si pensi al licenziamento, per un post, dell'operaio tarantino) e che, una volta immesso nel *web*, è quasi impossibile recuperare e "oscurare" ove lo si volesse.

Più tracce di noi lasciamo in rete, più ci condanniamo a servitù (solo apparentemente volontarie), esponendoci all'azione di chi voglia colpirci, ad esempio, con il *deep nude* o con altre forme di contenuti "*fake*".

Questi rischi sono, per i minori, amplificati dalla loro scarsa consapevolezza delle implicazioni di ogni loro "click", ma anche dall'effetto che ogni lesione dell'immagine o della dignità ha su una personalità più fragile, ancora in formazione.

La via della consapevolezza è necessaria per non privare i minori, almeno ultra14enni, di una socialità che oggi si esprime anche in questi modi, conferendo loro, tuttavia, anche gli strumenti indispensabili per orientarsi in un contesto che altrimenti è davvero troppo "più grande" di loro.

4. Libertà personale, tecnica e dignità.

Le applicazioni dell'intelligenza artificiale - per le quali la *Bozza* di regolamento europeo propone un'articolata disciplina per promuoverne uno sviluppo "conforme ai valori dell'Unione" - sono sempre più rilevanti dal punto di vista quantitativo e qualitativo.

Ad esse e alla loro pretesa neutralità si affidano decisioni significative, assecondando quella che Eric Sadin definisce "svolta ingiuntiva della tecnica", sempre più demiurgica, predittiva e quindi performativa, che rischia di privarci della "vertigine della libertà" (Kierkegaard).

Ciò induce, spesso, a sottovalutare i rischi derivanti dall'inclusione, nel processo algoritmico, di inferenze viziate dalle stesse precomprensioni da cui le macchine ci avrebbero dovuto liberare.

Quando poi i *bias* discriminatori caratterizzano – come la cronaca in particolare statunitense ha dimostrato - algoritmi utilizzati, anche solo in parte, nell'esercizio della potestà punitiva, i rischi che ne conseguono diventano ancor più intollerabili.

Queste considerazioni, tra le altre, sono sottese agli stringenti limiti posti dalla *Bozza* di regolamento al ricorso al riconoscimento facciale in luoghi pubblici da parte delle autorità di contrasto, idoneo più di altri a degenerare in forme di sorveglianza di massa, di cui quelle cinesi – con i loro sistemi di rilevazione persino delle emozioni – sono espressione significativa.

Lo stesso d.lgs. 51 del 2018 ha valorizzato, anche con specifiche norme incriminatrici, l'esigenza di prevenire implicazioni discriminatorie dell'intelligenza artificiale e di circondarne, comunque, l'uso in ambito di polizia con garanzie essenziali per la dignità e per la libertà della persona.

Sulla base di questi presupposti, il Garante ha ritenuto inammissibile l'attivazione, per fini di sicurezza pubblica, di un sistema di riconoscimento facciale carente di previsione normativa adeguata e delle correlative garanzie rispetto alla sorveglianza indiscriminata suscettibile di conseguirne.

L'estensione, potenzialmente indeterminata, dell'ambito della rilevazione biometrica avrebbe infatti comportato un netto cambio di paradigma nell'attività di contrasto.

Esso avrebbe dunque necessitato quantomeno di un'univoca previsione normativa, in grado di ricondurre misure altrimenti massive nel solco del canone di proporzionalità, circoscrivendone l'ambito sulla base di specifiche esigenze di prevenzione ed evitando che la tecnica divenga strumento di possibile discriminazione nei confronti dei soggetti più fragili.

Del resto, se i termini sono gli analizzatori dei tempi, quasi *signa temporum*, la vulnerabilità s'iscrive a pieno titolo nel loro nòvero.

La vulnerabilità designa persone, fenomeni e situazioni per i quali si evoca il concetto di ferita, di lesione, sia dal punto di vista fisico che da quello psicologico.

E tuttavia, il problema non si può risolvere nell'identificazione del gruppo o della categoria che assorbe tutti gli interessi che fanno capo a coloro che vi appartengono, ma piuttosto bisogna rivalutare la specificità della persona e dei suoi interessi, spirituali e materiali.

Si tratta, in sostanza, di guardare all'*homme situé*, alla persona in situazione, alla persona concreta ed alle esigenze che in concreto prospetta.

E' il passaggio dal soggetto – astratto, espresso in una categoria – alla persona.

E proprio la tutela delle persone vulnerabili – nelle forme più tradizionali e in quelle, più recenti, indotte dalla tecnica – ha rappresentato il tratto caratterizzante l'attività del Garante in questo primo anno e auspichiamo possa contraddistinguere l'intero nostro mandato, nella direzione di una civiltà digitale inclusiva.

La protezione dei dati può rappresentare, infatti, un prezioso strumento di difesa della persona da vecchie e nuove discriminazioni e di riequilibrio dei rapporti sociali, nella direzione dell'eguaglianza e della pari dignità sociale indicate dalla nostra Costituzione.

In questo senso, la protezione dei dati si sta dimostrando anche e sempre più determinante per un governo sostenibile della tecnica; perché la democrazia non degeneri, in altri termini, in algocrazia.