ISSN 1826-3534

federalismi.it
RIVISTA DI DIRITTO PUBBLICO ITALIANO, COMPARATO, EUROPEO

3 LUGLIO 2019

Il regolamento europeo sulla privacy: confini, sovranità e sicurezza al tempo del web

di Claudia Sartoretti
Professore associato di Diritto pubblico comparato
Università degli Studi di Torino

Il regolamento europeo sulla privacy: confini, sovranità e sicurezza al tempo del web *

di Claudia Sartoretti
Professore associato di Diritto pubblico comparato
Università degli Studi di Torino

1. Introduzione: il concetto di *privacy* nel nuovo "capitalismo della sorveglianza"

Il nuovo, complesso regolamento europeo sulla *privacy,* in vigore dal 25 maggio 2016 ed entrato in piena applicazione dal 25 maggio 2018, ha imposto nuove regole con le quali le istituzioni europee hanno voluto rispondere a un'esigenza sempre più impellente, emersa in modo chiaro e inequivocabile con il caso *Cambridge Analytica* che, nel marzo 2018, ha scoperchiato un mondo nel quale la circolazione dei dati personali è risultata essere al centro di flussi commerciali importantissimi. Il caso, nello specifico, sembra aver chiarito una volta per tutte come hanno fatto Facebook e altri social media a rimanere gratuiti e a fatturare allo stesso tempo ingenti quantità di dollari: essi sono ritenuti responsabili di aver "lucrato" sull'identità dei loro utenti, vendendo a società che ne hanno fatto gli usi più disparati (una fra queste la *Cambridge Analytica*, azienda di consulenza e per il marketing online) il profilo dei loro fruitori, i quali, a loro volta, nella maggioranza delle ipotesi, hanno sostanzialmente accettato il sistema senza esserne davvero pienamente consapevoli.

Sempre più spesso siamo oggetto di "attenzioni" costanti non solo da parte di servizi segreti o apparati statali, ma di un'industria che ha assunto proporzioni globali, in grado di lucrare sulle informazioni riguardanti i nostri comportamenti, ricavando profitti miliardari dalla trasformazione dei dati posseduti.

Da tempo si è avvertita la necessità nel Vecchio Continente di disciplinare i rischi della sorveglianza digitale, un bisogno che si è oggi acuito di fronte ad uno sviluppo delle tecnologie dell'informazione e della comunicazione che ha di fatto mutato la percezione che si ha degli individui, i quali vengono

* Articolo sottoposto a referaggio.

percepiti sempre meno cittadini e consumatori e sempre più identità "digitali", a guisa di blocchi di dati da cui traspaiono tutte le abitudini che li caratterizzano.

Il regolamento n. 2016/679 costituisce dunque l'ultima tappa di un cammino che a livello comunitario (oggi europeo) ha preso avvio da tempo, a partire dalla fine degli anni Novanta con la nota direttiva 65/96, adottata il 24 ottobre 1995, con il precipuo scopo di armonizzare il livello di tutela dei diritti delle persone riguardo al trattamento di dati personali. L'esigenza di armonizzazione nasceva dalla frammentazione in materia tra i diversi paesi aderenti all'Unione, per cui si è reso necessario procedere ad un ravvicinamento delle normative nazionali che non determinasse un indebolimento della tutela delle persone, ma anzi garantisse per tutti di Stati un elevato grado di tutela[1].

A partire dal momento in cui il processo di integrazione europea inizia a guardare oltre il mercato unico, verso l'orizzonte assai più ampio dei diritti della persona, sorge infatti la necessità di regolare il trattamento delle informazioni personali non solo in funzione di una maggior circolazione delle medesime che favorisca l'integrazione dell'economia europea, ma anche allo scopo di introdurre un elevato e coerente livello di protezione della riservatezza delle persone fisiche.

Un'evoluzione sul piano normativo che si accompagna anche all'evoluzione dello stesso concetto di "*privacy*", originariamente inteso come "diritto ad essere lasciato solo", secondo la tradizionale definizione con cui Warren e Brandeis[2], a fine Ottocento, formalizzarono per la prima volta a Boston l'esistenza di questo nuovo diritto, e progressivamente venuto ad arricchirsi di un nuovo significato riconducibile piuttosto alla capacità di autodeteterminazione informativa che un individuo acquisisce là ove gli si consenta di essere indipendente e di poter, conseguentemente, scegliere senza subire condizionamenti esterni che gli derivino dall'utilizzo e controllo di informazioni personali ad opera di terzi (sia privati che pubbliche amministrazioni).

Le stesse differenti locuzioni (*intimidad*, *vie privée*, riservatezza, *privatsphäre* e così via)[3], impiegate, in modo non propriamente omologo ed equivalente, dagli ordinamenti giuridici per dare rilievo a una nuova

[1] L'intervento armonizzatore europeo si inseriva in un contesto caratterizzato da una forte disomogeneità nella protezione dei dati personali. Se la gran parte degli ordinamenti europei si era infatti dotata di normative in attuazione della citata Convenzione di Strasburgo del 1981 – particolarmente interessante il *Data Protection Act* inglese del 1984 –, in altre esperienze, tra cui l'Italia, perdurava una situazione di totale vuoto normativo, che dottrina e giurisprudenza stentavano a colmare. La direttiva del 1995 ha rappresentato pertanto un significativo punto di riferimento nella materia tanto all'interno che al di fuori dell'ambito europeo.

[2] S.D. WARREN - L.D. BRANDEIS, *The Right to Privacy*, in *Harvard Law Review*, n. 5., vol. 4, 1890, pp. 193-220.

[3] Vedi, per tutti, sull'argomento, G. GIACOBBE, *Il diritto alla riservatezza in Italia,* in *Diritto e società,* 1974, p. 773; ID, voce *Riservatezza (diritto alla),* in *Enciclopedia del diritto,* vol. XL, Milano, 1989, p. 1243, il quale fa notare come, all'ambiguità terminologica che ha visto dottrina e giurisprudenza impiegare, nei vari ordinamenti giuridici, espressioni differenti e non propriamente omologhe per tradurre l'anglosassone "*privacy*", corrisponda un'altrettanta incertezza, oltre che difficoltà, a definire in modo chiaro e preciso il contenuto di questo nuovo

situazione giuridica soggettiva che consentisse di proteggere il singolo da indebite intrusioni all'interno delle mura domestiche, sono state in una qualche misura rivisitate e interpretate estensivamente – quando non anche sostituite dalla più generica e onnicomprensiva (o tale ritenuta) espressione "*privacy*" – per consentire loro di abbracciare le nuove necessità che la tutela della sfera intima di ciascun individuo ha progressivamente imposto.

Si noti poi che se i moderni mezzi comunicazione hanno permesso ai singoli individui di fruire di spazi di libertà (soprattutto di espressione e informazione) più ampi che in passato, essi hanno però anche finito per snaturare il concetto stesso di trasparenza, che da "mezzo", quale deve essere per raggiungere obiettivi superiori, strettamente connessi all'ideale democratico, è venuto piuttosto a configurarsi come un fine in sé, da perseguire anche a rischio di "paralizzare" i sistemi di protezione del segreto legittimo[4].

Oggi poi, in quella che si può definire l'era degli algoritmi in cui si è affermato di fatto un modello di organizzazione senza controlli burocratici classici, ma guidato piuttosto da codici e algoritmi, si assiste ad una ancor più crescente concentrazione del potere globale nelle mani di pochissime multinazionali che offrono servizi in cambio dei nostri dati.

Il problema che nasce è quello di una "monetizzazione dei dati personali" con la quale numerose persone finiscono per utilizzare i servizi e le applicazioni di Facebook, Google e così via in modo gratuito, non rendendosi probabilmente nemmeno conto di come in realtà "paghino" queste loro fruizioni alla multinazionale, attraverso la cessione di informazioni personali attraverso le quali è possibile dedurre comportamenti, abitudini, attitudini, preferenze e addirittura opinioni e sentimenti.

In questo scenario appaiono dunque necessari interventi di regolamentazione che permettano di limitare i danni di quella che, per l'economista Shoshana Zuboff[5], è una nuova specie di capitalismo (il c.d. "capitalismo della sorveglianza"), nella quale cambiano le "regole del gioco" e le dinamiche di domanda ed offerta che per anni hanno assicurato la democrazia di mercato. Al posto della nostra forza lavoro,

diritto. Cfr., altresì A. MILLER, *The assault on privacy. Computers, Data Banks and Dossiers,* Ann Arbor, 1971, p. 25, che già negli anni Settanta osservava come la *privacy* fosse in vero un concetto «*exasperatingly vague and evanescent*»

[4] Come ci rammenta invece M. RAVERAIRA, voce *Segreto nel diritto costituzionale,* in *Digesto discipline pubblicistiche,* vol. XIV, Torino, 2000, p.22 «il soggetto privato è tanto più (democraticamente) libero quanto più ne venga [invece] tutelato il diritto alla riservatezza», e cioè quel suo "spazio vitale" che – come ci ricordava S. RODOTÀ, *Privacy, libertà, dignità. Discorso conclusivo della Conferenza internazionale sulla protezione dei dati*, 26° Conferenza Internazionale sulla *Privacy* e sulla Protezione dei Dati Personale Wroclaw (Polonia), 14, 15, 16 settembre 2004, consultabile sul sito www.garanteprivacy.it – costituisce uno strumento necessario a difendere la *società della libertà* e a contrastare le spinte verso la costruzione di una società della sorveglianza, della classificazione, della selezione sociale.

[5] S. ZUBOFF, *The age of surveillance capitalism. The Fight for the Future at the New Frontier of Power,* New York, 2019; Id, *Facebook, Google and a dark age of surveillance capitalism*, in *Financial times*, 25 gennaio 2019, osserva testualmente: «*It soon became clear to me that surveillance capitalism diverged from many norms and practices that define the history of capitalism, especially the history of market democracy. Something startling and unprecedented had emerged and its consequences will shape the moral and political milieu of 21st-century society and the values of our information civilisation*».

che contraddistingueva il capitalismo industriale, il nuovo "capitalismo della sorveglianza" si nutre infatti di ogni aspetto dell'esperienza esperienza umana rapportata a materiale grezzo da tradurre in un insieme di dati comportamentali e da cui ricavare ricchi profitti. Seppure alcuni dei dati siano applicati per migliorare i servizi, il resto è, infatti, dichiarato come una "eccedenza comportamentale" ed è utilizzato per processi manifatturieri avanzati noti come *machine intelligence* e fabbricati poi in prodotti in grado di prevedere e anticipare quello che prima o poi faremo. I capitalisti della sorveglianza hanno infatti scoperto che la modifica del comportamento e gli interventi in tempo reale mediati digitalmente spingono i consumatori nella direzione desiderata da quegli stessi capitalisti.

L'accumulo senza precedenti di informazioni personali da parte delle multinazionali *hi-tech* ha però finito per creare un ordine economico da cui si è originata una nuova forma di disuguaglianza, derivante da squilibri nella "conoscenza", fra osservatori e osservati, in cui i primi sanno tutto dei secondi, mentre questi ultimi nulla conoscono del *modus operandi* dei primi.

Questa asimmetria, in cui aziende come Facebook, Google e così via beneficiano di una crescita del loro potere e delle loro ricchezze derivante dalla conoscenza che l'accumulo dei dati personali degli utenti consente loro, rischia chiaramente di annullare i diritti fondamentali associati all'autonomia individuale e come abbisogna di essere arginata, *in primis* attraverso una più efficace ed efficiente regolamentazione dei meccanismi che sono propri di questa nuova forma di capitalismo. Una necessità che l'Europa sembra aver ben compreso, come dimostra l'adozione del GDPR con cui l'Unione è intervenuta nel tentativo di iniziare ad arginare questo pericoloso sfruttamento delle previsioni comportamentali, derivante dalla sorveglianza costante degli utenti.

2. *Segue.* Verso una nuova regolamentazione del diritto alla *privacy*.

In Europa, il timore che l'elaborazione di banche dati automatizzate potesse essere utilizzata per controllare i propri cittadini, ha spinto inizialmente molti Stati europei, a cominciare dalla Francia e dalla Germania[6], ad adottare già tra gli anni '70 e '80 alcune normative riguardo al trattamento dei dati personali.

[6] La Germania è stato uno dei primi Paesi europei a varare leggi sulla protezione dei dati personali. Nella fattispecie, va segnalata la legge approvata dal *Land* dell'Assia con cui, già nel 1970, si era voluto varare una normativa in grado di tutelare i lavoratori da schedature indebite e dalla conservazione, insieme al trattamento, di dati racchiusi in banche dati. Alla legge dell'Assia sono successivamente seguite, a livello locale, ulteriori leggi adottate da trentacinque altri *Länder* con cui si voleva disciplinare il "segreto dei dati" e, in anticipo rispetto al resto d'Europa, si prevedeva l'ingresso nelle istituzioni locali di un'autorità garante eletta dal Parlamento. A livello federale, il governo tedesco approva nel 1977 il *Bundesdatenschutzgesetz* o BDSG, sostituito dalla Legge per lo sviluppo dell'elaborazione e della protezione dei dati personali del 1990 a seguito della sentenza del 15 dicembre 1983 del *Bundesverfassungsgericht* (caso *Volkszählungsentscheidung*) con la quale il *BVerfG*, con notevole lungimiranza, intuì per prima le implicazioni e le ripercussioni che un'indiscriminata raccolta e gestione di dati personali potesse

Il quadro normativo che in Italia e in numerosi altri ordinamenti giuridici si è invece per lungo tempo presentato agli occhi degli studiosi è stato caratterizzato dall'assenza di una disciplina organica e dalla presenza, al contrario, di una molteplicità di prescrizioni normative settoriali bisognose di essere ricomposte ad unità. Ad essere mancata inoltre è stata una disciplina uniforme ed omogenea a livello comunitario atta a superare il divario esistente nei livelli di tutela dei diritti e delle libertà personali, garantiti dagli Stati membri con riguardo al trattamento dei dati personali e tale da permettere un ravvicinamento delle legislazioni nazionali applicabili in materia che garantisse un più elevato grado di tutela nella Comunità. Colmare questo scarto a livello normativo è apparsa altresì una condizione necessaria a eliminare qualsivoglia impedimento alla trasmissione di dati fra ordinamenti che possa fungere da ostacolo all'esercizio di attività economiche a livello europeo.

La creazione e il rafforzamento di un mercato unico costituisce da sempre una priorità per il Vecchio Continente e l'intervento del legislatore europeo con la direttiva 95/46, considerata una vera e propria pietra miliare in tema di protezione dei dati personali in Europa, una sorta di direttiva-madre, ha mirato, non casualmente, a stabilire un giusto equilibrio fra un livello elevato di tutela della vita privata delle persone e la libera circolazione dei dati personali all'interno dell'Unione europea (UE), fissando limiti precisi per la raccolta e l'utilizzazione dei dati personali e chiedendo a ciascuno Stato membro di istituire un organismo nazionale indipendente incaricato della sorveglianza di ogni attività associata al trattamento dei dati personale.

Da questo momento in avanti la sensibilizzazione verso i problemi riguardanti il trattamento delle informazioni personali e la tutela della *privacy* è risultata in continua ascesa nell'ordinamento comunitario e, conseguentemente, in quello degli Stati membri. Ne è una dimostrazione il successivo riconoscimento

rappresentare in termini di lesione dei diritti fondamentali della persona. Nella sua decisione, il *BVerfG* ha attribuito inequivocabilmente alla tutela dei dati personali un rilievo costituzionale, individuando per la prima volta un "diritto all'autodeterminazione informativa", configurato come una forma di concretizzazione del diritto generale della personalità di cui agli artt. 1 e 2 della Legge Fondamentale Tedesca, che tutelano rispettivamente la dignità umana e i diritti di libertà della persona. Sul punto, per una ricostruzione storica, cfr., *ex multis,* A. CERRI, voce *Riservatezza (diritto alla) II) Diritto comparato e straniero,* in *Enciclopedia Giuridica Treccani,* Roma, 1991; L. REISINGER, *La protezione dei dati personali nell'esperienza internazionale. Repubblica Federale di Germania: la critica alle teorie delle sfere,* in AA.VV., *Banche dati e diritti della persona,* Padova, 1985. p. 95; J. LEE RICCARDI, *The German Federal Data Protection Act of 1977: Protecting the Right to Privacy?,* in *Boston College International and Comparative Law Review,* n. 1, vol. 6, 1983, p. 243.
L'ordinamento francese consacra invece per la prima volta con la legge del 17 luglio 1970 n.643 il diritto alla vita privata, riconoscendo espressamente all'art. 9 del *code civil* il diritto di ciascuno alla vita privata, e adotta una normativa sul trattamento dei dati personali nel 1978 (*Loi relative à l'informatique, aux fichiers et aux liberté*), mostrando di comprendere sin da subito i contorni nuovi e inediti assunti dalla problematica concernente la tutela della *privacy*. Sull'argomento e, nella fattispecie, sull'evoluzione della normativa francese in tema di protezione dati personali, sia consentito rinviare a C. SARTORETTI, *Contributo allo studio del diritto alla* privacy *nell'ordinamento costituzionale. Riflessioni sul modello francese,* Torino, 2008, a cui si rinvia altresì per ulteriori riferimenti bibliografici.

della protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale come un diritto fondamentale, affermato *in claris verbis* dall'art. 8 par. 1, della Carta dei diritti fondamentali dell'Unione europea – c.d. Carta di Nizza – e dall'art. 16, par. 1, del Trattato sul funzionamento dell'Unione europea (TFUE), i quali, da un lato, stabiliscono espressamente che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano, dall'altro, mantengono questa situazione soggettiva distinta dal tradizionale diritto al rispetto della vita privata e familiare, del domicilio e della corrispondenza disciplinato all'art. 7 della medesima Carta [7].

Come è stato osservato, i diritti sono soliti assumere le coloriture storiche, sociali e culturali delle diverse società ed epoche storiche che si susseguono, «rivendicando sempre nuovi modi di essere nel presente»[8], il che li rende poco inclini ad essere fissati in un'identità rigida o ad essere affidati ad una forma certa, poiché consegnati alla storicità che riguarda non solo il loro "divenire", ma persino il loro "essere". Lo stesso catalogo dei diritti – è stato inoltre evidenziato[9] – appare soggetto a continue variazioni, integrazioni e correzioni, che non necessariamente lasciano traccia nei documenti costituzionali.

Il diritto alla *privacy* risulta per certi versi particolarmente sensibile all'evoluzione storico-tecnologica e sembra nel presente rivendicare più di altre situazioni giuridiche soggettive nuovi modi di essere, come dimostra la sua intrinseca pluralità contenutistica e la sua forte dinamicità che lo fanno apparire come una sorta di *work in progress,* la cui tutela deve essere costantemente adeguata rispetto alla incessante sequenza di innovazioni tecnologiche e sociali[10].

Come è stato notato, il cambiamento tecnologico non è invero mai mancato in alcuna epoca, anche se il suo ritmo e la sua entità sono risultati sovente discontinui[11]; tuttavia ciò che si può recentemente rilevare è una decisiva accelerazione impressa dalla tecnologia alle trasformazioni del vivere quotidiano sia

---

[7] La Carta dei diritti, in questo modo, pone l'accento sulla complessa portata del concetto di *privacy* capace di esprimere nuovi ed ulteriori significati che si sommano a quello che costituisce il nucleo originario del diritto alla riservatezza (il c.d. *right to be let alone*) e permettono di dare nuove risposte a nuovi problemi e necessità che il progresso economico, tecnologico e sociale ha creato e continua progressivamente a creare. Per un commento, cfr., *ex multis,* F. DONATI, *Protezione dei dati personali,* in R. BIFULCO – M. CARTABIA – A. CELOTTO (a cura di), *L' Europa dei diritti. Commento alla Carta dei diritti fondamentali dell'Unione Europea*, Bologna, 2001, p. 83; J. RIDEAU, *Droit institutionnel de l'Union et des Communauteés européennes*, Paris, 2006, p. 349; F. PICOD - S. Van DROOGHENBROECK, *Charte des droits fondamentaux de l'Union européenne: Commentaire article par article,* Bruxelles, 2018; G. GONZÁLEZ FUSTER - R. GELLER, *The fundamental right of data protection in the European Union: in search of an uncharted right*, in *International Review of Law Computers & Technology,* n. 1, vol. 26, 2012, p. 73

[8] M.R. FERRARESE, *Il diritto al presente. Globalizzazione e tempo delle istituzioni*, Bologna, 2002, p. 140

[9] M.R. FERRARESE, op. loc. cit.

[10] A. GIDDENS, *Le conseguenze della modernità,* (1990), trad. it., Bologna, 1994, p. 115 sottolinea l'esistenza di una «trasformazione dell'intimità nei contesti della vita quotidiana» e rammenta come la globalizzazione non riguardi solo i grandi sistemi dell'ordine finanziario mondiale, né si esaurisce in un insieme di fattori esterni o distanti dall'individuo, ma rappresenta anche un fenomeno interno che influisce sugli aspetti intimi e personali della nostra vita, fino a riconfigurarne i tratti essenziali.

[11] Cfr., P. SHANKAR JHA, *The twilight of the Nation State: Globalisation, Chaos, And War,* London, 2006

nell'ambito privato che in quello pubblico e professionale. Si potrebbe parlare di una sorta di "quarta rivoluzione industriale" iniziata con la nascita e lo sviluppo delle banche dati elettroniche e con la strutturazione e crescita di sistemi informativi digitali, e sfociata in quelle dinamiche pervasive della rete che hanno cambiato qualitativamente il contenuto della *privacy*, rendendo anche necessario l'adattamento delle previsioni normative esistenti in modo da garantire un assetto *effettivo* di tutele che – al passo con l'evoluzione tecnologica – difenda, al tempo stesso, la sicurezza strategica delle infrastrutture e la protezione dei dati individuali (*Data Protection*)[12].

3. Le nuove tecnologie di informazione e comunicazione e i rischi della trasparenza "dell'intimità".

Lo sviluppo di Internet e di tutte le strutture ad esso connesse, non ultimi i social networks, e l'ampio uso che persone, ma anche aziende ed istituzioni ne fanno ha riproposto in termini ancora più forti l'urgenza di tutelare quel sottile equilibrio fra l'utilizzo delle nuove tecnologie, certamente molto vantaggiose, e la tutela dei dati che vengono utilizzati e trasmessi tramite i canali digitali.

Nella illusoria convinzione che la rete costituisca uno strumento intrinsecamente (cioè per natura) democratico e che disporre di più informazioni permetta automaticamente di essere più liberi, le persone trascorrono sempre più tempo sulla rete e trasmettono un numero sempre maggiore di informazioni personali, ignorando o sottovalutando i pericoli che si insidiano in quello che, all'apparenza, sembra essere uno spazio di espressione aperto, libertario e quasi anarchico. "Inebriati" dall'idea di poter attingere senza impedimenti a ogni genere di conoscenze, notizie e informazioni e di poter usufruire di tecnologie che permettono a tutti di altrettanto liberamente comunicare, esprimere le proprie opinioni, idee ed emozioni, e di costruire una comunità senza confini, i consumatori/utenti della rete sembrano aver smarrito nella "quotidianità virtuale" quel senso di responsabilità e quella prudenza che hanno accompagnato invece il loro agire nella vita reale.

Già nel 1975, Michel Foucault[13] metteva però in guardia dai rischi, sovente trascurati, derivanti dalla consapevolezza di essere o anche solo poter essere osservati. Il *Panopticon*, il carcere progettato da Jeremy Bentham e ripreso dal pensatore francese come figura rappresentativa del potere nella società contemporanea, sembra quasi creato ad arte per costituire una metafora del web e del suo lato oscuro di

[12] U. GASSER, *Law, privacy & technology commentary series recoding privacy law: reflections on the future relationship among law, technology, and privacy recoding* in *Harvard Law Review*, n. 2, vol. 130, 2016, p 61, evidenzia come «*the history of privacy is deeply intertwined with the history of technology*», sottolineando che «*a wealth of scholarly literature tracks and demonstrates how privacy as a normative concept has evolved in light of new information and communication technologies since the early modern period, when face-to-face interactions were challenged by urbanization and the rise of mass communication*»

[13] M. FOUCAULT, *Sorvegliare e punire. Nascita della prigione,* (1975), trad. it., Torino, 1993.

dominio: ai nuovi apparati digitali sembrano infatti potersi porre le stesse domande di fondo che Foucault rivolgeva cinquanta anni fa ai dispositivi disciplinari[14]. Ad accomunare i moderni sistemi di controllo "digitale" alle forme di sorveglianza imposte dalla società disciplinare è la condivisione della motivazione sociale che spinge in un caso come nell'altro i cittadini a sottomettersi volontariamente al potere. Secondo Foucault la ragione di fondo della accettazione ad essere sorvegliati è, nella modernità, la ricerca di sicurezza, che porta a rinunciare a porzioni di libertà in cambio di rassicurazioni sulla propria vita e il proprio benessere. In modo non del tutto dissimile si potrebbe concludere che l'odierna esposizione sulla rete di noi stessi, di informazioni su di noi, di immagini, storie, pensieri e opinioni che ci riguardano, rappresenti una sorta di congruo prezzo che si è consapevolmente disposti a pagare per poter avere a disposizione relazioni, informazioni, immagini e pensieri di altri.

La rete però si rivela però un luogo ricco di insidie e quella sorveglianza a cui ci sottoponiamo ormai regolarmente oltre che scientemente, allorché optiamo di mettere a nudo le nostre identità sul web, finisce per rimettere al centro della questione la sicurezza, ma in una dimensione, questa volta, prettamente "individuale", e cioè come sicurezza dei propri dati, che va garantita solo con l'adozione di efficaci strumenti di garanzia per la *privacy*, in grado di sottrarre la persona alla «dittatura dell'algoritmo»[15]. Alle tecnologie dell'informazione e della comunicazione – ci ricorda Stefano Rodotà[16] – è stato riconosciuto il merito di rendere la società più trasparente, rendendo possibile il controllo diffuso sul potere, *rectius,* su qualsiasi potere. Quando però l'algoritmo diviene il fondamento stesso del potere esercitato da un soggetto, com'è nel caso evidente di Google, e tutto ciò che lo riguarda è avvolto dalla massima segretezza, allora si finisce per essere verosimilmente dinnanzi ad una nuova versione degli *arcana imperii*, che non soltanto tutelano l'attività d'impresa, ma si impadroniscono anche, direttamente o indirettamente, della vita e dell'intimità stesse delle persone[17].

Nello spazio "liquido" di Internet i cittadini diventano infatti una sorta di patrimoni informativi fluidi sottoposti alla sovranità della tecnocrazia delle maggiori piattaforme digitali persistenti on line (Google, Facebook, Apple), le quali, attraverso il controllo dei dati personali che circolano in rete, si assicurano, di fatto, il potere di governo sulle vite digitali di ciascuno di noi. Facebook, Google, ma anche

[14] Vedi , F. COLOMBO, *Controllo, identità, parresia. Un approccio foucaultiano al web 2.0* in *Comunicazioni sociali*, n. 2, 2012, pp. 197-212

[15] Così, S. RODOTÀ, *Il mondo nella rete: quali i diritti, quali i vincoli*, Roma-Bari, 2014, p. 33

[16] S. RODOTÀ, *op. loc. cit.*

[17] G. FIORIGLIO, *Sorveglianza e controllo nella società dell'informazione. il possibile contributo dell'etica* hacker, in *Nomos,* n., 2014, p. 1, osserva come nella odierna società della sorveglianza e del controllo, infatti, vi sia un problema molto delicato, connesso sia ai software proprietari che ai servizi informatici: la trasparenza è molto rara e mentre l'interazione con gli strumenti tecnologici si semplifica, internamente i medesimi sono sempre più oscuri e complessi, al di fuori della portata dell'uomo medio, che anche da questo punto di vista è sempre più "di vetro".

Uber, Twitter e così via, hanno infatti scoperto come trasformare le informazioni riguardanti la nostra quotidianità in una sorta di "prodotti predittivi", capaci di anticipare le nostre azioni, e da offrire a chiunque sia disposto a pagare per possedere questa nuova ricchezza.

Una tale diffusione di informazioni personali all'interno di uno spazio in continua mutazione, senza regole, che procede a folle velocità e dove ogni singola azione individuale è tracciata e tracciabile, ha reso ancor più difficile la coniugazione fra il diritto di "tutti" all'informazione e quello del singolo alla sua *privacy*, soprattutto perchè il primo è sembrato in alcuni momenti quasi sovrastare il secondo, in un bilanciamento che sa forse più di una scala gerarchica in termini di valore dato e attenzione prestata a due differenti esigenze che di un equo contemperamento fra situazioni soggettive egualmente meritevoli di tutela. Come un Giano bifronte, il villaggio globale e gli strumenti tecnologici che ne hanno consentito lo sviluppo, presentano invece tanto aspetti di positività che di negatività, come sembrano confermare i rischi – sempre più frequenti ed elevati – di intrusione nella vita privata degli individui aventi accesso alla rete, dando origine a una sorta di nuova tirannia, quella della trasparenza e della gratuità delle informazioni a cui tutti possono ora accedere[18]. Se le nuove tecnologie web hanno, infatti, certamente rappresentato una svolta epocale sotto il profilo dell'informazione e della comunicazione, accelerandone i processi di acquisizione, nel primo caso, e offrendo nuovi canali di propagazione nel secondo, le distorsioni nel loro utilizzo (si pensi, ad esempio, al furto di identità o alla questione di come assicurarsi la cancellazione di dati personali una volta che si è stabilito di voler uscire da un social network, disattivando il proprio account, visto che le informazioni e i materiali inseriti online permangono all'interno degli archivi informatici dell'azienda che offre il servizio) ci obbligano, invece, a riperimetrare la libertà di accesso alla rete e a disciplinare quel difficile equilibrio/squilibrio fra libertà di espressione e diritto alla privacy che si è venuto ad originare, ridefinendo le frontiere della protezione dei dati personali e tutelando il già compromesso diritto degli individui di autodeterminarsi negli spazi digitali.

Se infatti, come è noto, sul piano fisico, la sovranità su di sé e sul proprio corpo è garantita e tutelata dal diritto di *habeas corpus*, locuzione contenuta già nella *Magna Charta Libertatum* (1215) ed esplicitata nell'*Habeas Corpus Act* (1679), e tradotta oggi nel principio costituzionalmente ed universalmente riconosciuto dell'inviolabilità della libertà personale, il suo corrispettivo nella società digitale – l'*habeas data* – seppur codificato nella Carta di Nizza, abbisogna invece di nuove e più efficaci regole che consentano di soddisfare le nuove e multiformi esigenze di tutela della *privacy* che la tecnologia in continuo e rapido divenire fa affiorare incessantemente.

[18] Per un approfondimento sul punto, cfr. L. BOURGORGUE-LARSEN, *Les nouvelles technologies,* in *Pouvoirs*, n. 130, 2009, p. 65

Da tempo si rivendicano infatti il riconoscimento e un'adeguata difesa della sovranità digitale, intesa come possibilità di ciascun individuo di controllare, *de jure* e *de facto,* uno spazio che, seppur privo di materialità (non siamo infatti in presenza di un territorio in senso fisico), non è meno meritevole di protezione, come dimostra, ad esempio, il recente ed esplicito richiamo ad esso e alla necessità di incrementarne la tutela contenuto in un documento interno del Ministero dei Trasporti tedesco, il cui contenuto è stato rilevato il 20 marzo 2017 dal quotidiano *Die Welt*.

La decisione della Corte di Giustizia UE nel caso *Schrems*[19] a sua volta rivendica la necessità di poter difendere la sovranità digitale della stessa Unione europea, riconoscendo alle istituzioni europee la piena giurisdizione sul trattamento dei dati personali dei cittadini europei e sancendo l'invalidità dell'accordo commerciale sul regime dell'approdo sicuro (c.d. *safe-harbour*), precedentemente stipulato con gli Stati Uniti, con il quale, fino ad allora, si era consentito alle aziende americane di manipolare e transitare i dati personali dei loro utenti europei su server americani.

Contravvenendo così a quella idea originaria che internet e tutte le attività in rete costituiscano ambiti a-territoriali e, come tali, non soggetti a sovranità statale [20], la Corte, chiamata a pronunciarsi su una disputa che riguardava proprio l'ambito "spaziale" del web, ha, nella fattispecie, restituito a internet dei confini fisici suoi propri, riconoscendo che i dati personali, quand'anche non siano direttamente connessi ad uno specifico territorio, restano tuttavia legati alla cittadinanza[21] intesa in senso tradizionale. Ad essere rilevante nel mondo virtuale, infatti, non è solo il concetto nuovo di cittadinanza digitale che rimanda a un complesso di diritti e doveri dei cittadini formulati in adattamento allo sviluppo dell'*e-government* e della

[19] Corte di giustizia, sentenza del 6 ottobre 2015, causa C-362/14, *Schrems*, relativo alla competenza giurisdizionale nelle controversie promosse dall'utente di un social network ed il gestore della piattaforma. In sintesi, la causa principale riguardava la controversia promossa contro Facebook da un utente austriaco, attivista nel campo della tutela della *privacy* sui social network, in relazione all'illecito trattamento dei dati personali sul social network.
Si osservi come già a partire da caso *Google Spain* (Corte di giustizia, sentenza 13 maggio 2014, causa C-131/12, *Google Spain, Google Inc. e Agencia Española de Protección de Datos (AEPD), Mario Costeja González*), si può apprezzare il tentativo della Corte di ampliare l'ambito di applicazione territoriale della direttiva 95/46/CE, attraverso un'interpretazione estensiva dell'art. 4, per assicurare ai dati di cittadini europei, trattati fuori dai confini dell'Unione, le medesime garanzie assicurate ai trattamenti dei dati effettuati all'interno dell'Unione. Vedi, per un commento, *ex multis,* G. FINOCCHIARO, *La giurisprudenza della Corte di Giustizia in materia di dati personali da Google Spain a Schrems*, in *Il diritto dell'informazione e dell'informatica*, fasc. 4-5, 2015, p. 779; F. PIZZETTI, *La decisione della Corte di Giustizia sul caso Google Spain: più problemi che soluzioni,* in *Federalismi.it,* n.12/2014; O. POLLICINO, *Un* digital right to privacy *preso (troppo) sul serio dai giudici di Lussemburgo? il ruolo degli artt. 7 e 8 della carta di Nizza nel reasoning di Google Spain*, in *Il diritto dell'informazione e dell'informatica,* 2014, p. 7

[20] Vedi, V. ZENO-ZENCOVICH, *Intorno alla decisione nel caso Schrems: la sovranità digitale e il governo internazionale delle reti di telecomunicazione*, in *Il diritto dell'informazione e dell'informatica,* n.4-5, 2015, p. 683

[21] Di avviso contrario, J. DASKAL, *The Un-Territoriality of Data*, in *Yale Law Journal*, n. 2, vol. 125, 2016, p. 326 che osserva come «*Data also challenges territoriality's twentieth-century companion criteria— citizenship and national ties—as determinative of the constitutional and statutory rules that apply*»; cfr. altresì, P. ZANINI, *Significati del confine: i limiti naturali, storici, mentali,* Milano, p. 63 che evidenzia come la cittadinanza rappresenti lo strumento attraverso il quale un governo regola, e soprattutto controlla, l'appartenenza di un individuo al proprio spazio civico.

fruizione dei servizi in rete, ma anche quella classica e formale nozione con la quale si vuole esprimere la condizione giuridica di quanti appartengono ad uno Stato in virtù di un particolare collegamento al suo territorio.

La mutevolezza che secondo la dottrina, non solo italiana[22], contraddistingue la categoria della cittadinanza ed i significati che quest'ultima assume nel concreto (in risposta anche e soprattutto ai cambiamenti sociali, politici ma altresì tecnologici) non escludono, infatti, che si possa ancora parlare di "cittadinanza" nel senso tradizionale – e caro a Santi Romano[23] - di "appartenenza", rinviando ad uno status giuridico che appare strettamente connesso a concetti quali "Stato" e "sovranità"[24].

Ed è sulla base di questa antica nozione che la Corte di giustizia, chiamata a decidere sulla controversia sorta dal fatto che, nonostante il 90% degli utenti di Internet viva fuori dagli Usa, i dati personali che li riguardano sono in America, custoditi nei server delle cinque maggiori aziende digitali del pianeta, sembra aver voluto ridefinire in modo più chiaro i confini della sovranità dell'UE sulle reti di telecomunicazione. Condannando il trasferimento di dati personali di *cittadini* europei verso gli Stati Uniti, il giudice europeo ribadisce la necessità di ripristinare una sorta di "confine", una separazione anche all'interno di uno spazio liquido quale è internet, rivendicando la competenza del diritto UE a regolamentare il trattamento delle informazioni personali, poiché, come ci ricorda la stessa direttiva 95/46, se "lo sviluppo degli scambi internazionali comporta necessariamente il trasferimento oltre frontiera di dati personali" e " la tutela delle persone garantita nella Comunità dalla presente direttiva non osta al trasferimento di dati personali verso paesi terzi che garantiscano un livello di protezione adeguato", non deve, per contro, essere consentito il trasferimento di dati personali verso un Paese terzo che non offra un livello di protezione adeguato.

Seppur poroso, quando non anche difficilmente percepibile, come appunto nel caso del cyberspazio, l'idea di confine torna così prepotentemente alla ribalta anche nel mondo digitale, e, anche quando correlato alla cittadinanza degli utenti/consumatori, più che a un elemento materiale come la terra, permette comunque all'Ue di iniziare a tracciare una linea di demarcazione atta a consentirle di esercitare

[22] Sul punto la letteratura è molto vasta, cfr., *ex. multis,* E. GROSSO, *Le vie della cittadinanza*, Padova, Cedam, 1997; G. AZZARITI, *La cittadinanza appartenenza, partecipazione, diritti delle persone*, in *Diritto Pubblico*, 2/2011, p. 425; P. HAEBERLE, *La cittadinanza come tema di una dottrina europea della Costituzione,* in *Riv. dir. cost.*, 1997, p. 19; W. LANCE BENNETT, *Changing Citizenship in the Digital Age*, in *Civic life online,* 2008; F. GREFFET - S.WOJCIK, *La citoyenneté numérique. Perspectives de recherche*, in *Réseaux*, n.2, 2014, p. 125; P. Costa, La cittadinanza: un tentativo di ricostruzione archeologica, in La cittadinanza. Appartenenza, identità, diritti, ed. D. ZOLO, Roma 1994, p. 48; J. BUTLER - G. C. SPIVAK, *Who Signs the Nation-State?*, London, 2009; P. MINDUS, *The Contemporary Debate on Citizenship*, *Revus*, Online, 9, 2009; K. RUBENSTEIN, *Citizenship in an Age of Globalisation: The Cosmopolitan Citizen*, in *Law Context: A Socio-Legal Journal,* n.25, 2007, p.88

[23] S. ROMANO, *Principi di diritto costituzionale generale,* Milano, 1947, p. 100

[24] P. COSTA, *Civitas. Storia della cittadinanza in Europa,* I, Roma-Bari, 1999, p. 3

la supremazia decisionale su una materia particolarmente sensibile come quella dei diritti fondamentali e di rivendicare il controllo della rete e la potestà di fissare le regole che governano le attività che vi si svolgono.

4. Alla ricerca di confini nella liquidità digitale.

In linea di continuità dunque con questa tendenza da parte delle istituzioni europee di recuperare sovranità all'interno di spazi immateriali, ancorché delimitati da frontiere prive di forma visibile, l'UE ha così approvato il recente regolamento sulla *privacy* con il quale ha voluto fare un altro passo avanti nel cammino di acquisizione di nuova sempre maggiore consapevolezza relativa alla società che stiamo vivendo dove i dati personali costituiscono ormai una merce di scambio e le violazioni della *privacy* risultano all'ordine del giorno. I problemi di Internet non possono più essere affrontati sulla base della tradizionale interpretazione libertaria, che vede la Rete come spazio intrinsecamente anarchico, per sua natura insofferente ad ogni regola, capace di ristabilire autonomamente la libertà violata.

L'obiettivo che l'Unione europea si è proposto è quello di regolare in modo uniforme tutti i flussi di informazioni che passano in Europa, cercando di riordinare per via legislativa il mondo digitale finora dominato dai colossi stranieri, soprattutto nord-americani. Nella fluidità e permeabilità dell'universo internet ove i dati e le identità individuali fluttuano senza sosta da un estremo all'altro del Pianeta, la maggiore difficoltà è stata sinora quella di assicurare una concreta ed efficace tutela della *privacy* anche laddove – come nella maggior parte dei casi – il flusso di informazioni raccolto in Europa confluisca in aziende straniere a cui appartiene il monopolio del trattamento

Chiarito già nel primo considerando che la protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale, il Parlamento ed il Consiglio si sono apprestati quindi a precisare nel regolamento l'ambito di applicazione territoriale, evidenziando come esso sia vincolante anche per i trattamenti di dati personali non svolti all'interno del territorio dell'Unione Europea, se relativi all'offerta di beni o servizi a cittadini residenti nella UE, o tali da consentire il monitoraggio dei comportamenti di interessati che si trovano in Unione europea (art.3, comma 2, Regolamento UE 2016/679).

Più precisamente, l'art.3, al primo comma, stabilisce la regola generale secondo cui il regolamento si applica a qualsiasi trattamento di dati personali effettuato nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento avvenga all'interno o all'esterno dell'Unione medesima. La nozione di stabilimento non è definita nel Regolamento, ma il considerando 22 specifica come lo stabilimento prescinda da una determinata forma giuridica: non è determinante la forma giuridica assunta, sia essa una

succursale o una filiale dotata di personalità giuridica. L'elemento qualificante è dunque l'effettivo e reale svolgimento di un'attività di trattamento dei dati personali all'interno di un'organizzazione stabile[25]. Nel secondo comma il legislatore europeo si preoccupa invece di arginare i rischi di un trattamento ad opera di titolari che non siano stabiliti in Europa e che come tali risponderebbe alla normativa nazionale del Paese di appartenenza, anziché a quella europea. Pertanto, «onde evitare che una persona fisica venga privata della protezione cui ha diritto in base al presente regolamento» (considerando n. 23) e optando per un approccio che guarda prima di tutto ai soggetti destinatari del servizio (i c.d. interessati), vengono così introdotti i due criteri sopra menzionati che costituiscono la vera novità del regolamento in esame e che consentono di estendere appunto l'applicazione del regolamento anche ai titolari non presenti sul territorio UE, allorché le loro attività siano connesse all'offerta di beni o servizi a persone interessate che si trovano in Europa, a prescindere dalla sussistenza di un'obbligazione di pagamento a carico di queste, o esse consistano nel controllo del comportamenti degli utenti sul territorio europeo, da accertare – secondo alcuni spunti interpretativi offerti dal considerando 23 della normativa in esame – verificando, ad esempio, se le persone fisiche sono tracciate su internet, compreso l'eventuale ricorso successivo a tecniche di trattamento dei dati personali che consistono nella stesura del profilo della persona fisica, finalizzate all'adozione di decisioni che la riguardano o analizzarne o prevederne le preferenze, la condotta e le posizioni personali.

Infine, va altresì aggiunta una terza opzione prevista dal terzo comma dell'art.3 in cui si fa riferimento al trattamento di dati personali effettuato da un titolare del trattamento medesimo che non è stabilito nell'Unione, ma in un luogo soggetto al diritto di uno Stato membro in virtù del diritto internazionale pubblico.

Pur confermando dunque il principio di stabilimento introdotto dalla direttiva 95/46 la nuova normativa ne circoscrive la portata, sancendo l'applicabilità della disciplina dettata dal regolamento "indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione" e stabilendo l'applicazione delle sue regole anche a titolari e responsabili non stabiliti nell'UE. Quindi, anche le società che si trovano al di fuori dell'UE, ma che tuttavia elaborano dati personali di soggetti che si trovano nel territorio dell'Unione europea (è irrilevante se cittadini, residenti o meno) nel contesto di attività di profilazione dovranno conformarsi alle norme del GDPR. Ed è in ciò che sta la vera portata innovativa

[25] In verità già con la sentenza del 1° ottobre 2015, causa C-230/14C-230/14, *Weltimmo*, la Corte di Giustizia europea ha sancito ulteriormente che la forma giuridica di stabilimento (cioè il rappresentante nel territorio nazionale) non è il fattore predominante per decidere sulla giurisdizione. Nei punti 25 e 27 della sentenza si legge in particolare che «l'espressione "nel contesto delle attività di uno stabilimento" non può ricevere un'interpretazione restrittiva» e che «il legislatore dell'Unione ha […] quindi previsto un ambito di applicazione territoriale della direttiva 95/46 particolarmente esteso, che ha inserito all'articolo 4 della stessa».

del regolamento: nel fatto che per la prima volta l'elemento che determina l'applicabilità delle norme in tema di trattamento dati si lega al luogo in cui è situato l'interessato.

In sostanza, se fino ad ora l'utente di uno Stato membro che acquistava online da un sito web con sede, ad esempio, negli USA doveva soggiacere alla legge del Paese di appartenenza (in questo caso statunitense), con il nuovo regolamento spetterà alle aziende americane ed altri soggetti stranieri che si propongono nell'area UE il compito di adeguarsi alla normativa europea se non vogliono essere sanzionati.

In questo modo, muovendosi nella stessa direzione tracciata dalla Corte di giustizia con il caso *Schrems*, gli organi legislativi europei hanno voluto rispondere in modo forte ed efficace al bisogno crescente di stabilire confini e delimitare un'area in cui all'Unione europea fosse consentito esercitare pieni e sovrani poteri, nella prospettiva di contribuire alla realizzazione di «uno spazio di libertà, sicurezza e giustizia e di un'unione economica» oltre che «al progresso economico e sociale, al rafforzamento e alla convergenza delle economie nel mercato interno e al benessere delle persone fisiche» (secondo considerando, Regolamento UE 2016/679).

Se compito principale dei confini è "separare" e tale funzione si fonda sulla necessità di stabilire contorni nitidi, indispensabili a mettere in ordine, organizzare e gestire un determinato ambito (non solo fisico) in modo da offrire maggiori tutele in termini di "sicurezza" a chi lo occupa, allora anche e a *fortiori* in uno spazio "liquido" come quello del web l'introduzione di riferimenti fissi e stabili contro la dilagante incertezza tipica della fluidità di questo mondo può apparire un fattore irrinunciabile [26].

Nella liquidità digitale, i confini assurgono a strumenti per conoscere e tenere sotto controllo (meglio, regolare) uno spazio virtuale, che non ha un luogo fisico in cui risiedere, ma esiste tuttavia realmente e cresce parallelamente all'avanzare del progresso e della tecnologia digitali. In questo "mondo nel mondo", quale è il cyberspazio, le possibilità di muoversi, conoscere e vedere si amplificano e lo spazio finisce quindi per dilatarsi senza limiti, generando il bisogno di stabilire nuove difese per chi decide di avventurarsi nell'ignoto e nell'incertezza che contraddistinguono la dimensione immateriale di internet[27].

---

[26] R. CROOTOF, *International cybertorts: expanding state accountability in cyberspace* in *Cornell Law Review,* vol. 103, 2018, p. 565 in cui si evidenzia come l'assenza di confini geografici del web ha fatto sorgere difficoltà in merito alla responsabilità degli Stati in merito ai danni derivanti da *cyberoperaziontions*. L'Autrice osserva infatti come questo fenomeno sia causato «*largely because classifications created in physical space do not map well onto the cyber domain*».

[27] G. SCACCIA, *Il territorio fra sovranità statale e globalizzazione dello spazio economico,* in *Rivista AIC,* n.3/2017 p. 1, ma spec., p. 19, osserva: «Se al tempo di Schmitt la crisi del νόμος veniva dal mare, oggi essa viene dallo spazio virtuale della Rete. In questo spazio, che come quello marino non può essere interamente occupato, né ripartito, si svolge la competizione economica e culturale per la conquista del potere sulla terra». Vedi, anche, S. ORTINO, *Il nuovo* Nomos *della Terra, Profili storici e sistematici dei nessi tra innovazioni tecnologiche, ordinamento spaziale, forma politica*, Bologna, 1999, p.24, il quale fa notare come: "Lo spazio cibernetico come lo spazio marino e lo spazio del nomade, non può essere né occupato, né ripartito, ma è parte del *nomos* planetario, in quanto diventa la via dell'espansione culturale, commerciale ed economica e il luogo della competizione e della spartizione della terra".

L'utilizzo di Internet ha certamente il merito di aver accorciato o addirittura annullato le distanze, oltre che a quello di aver abbreviato i tempi di trasmissione delle informazioni, rendendole accessibili ovunque e immediatamente; cionondimeno, intaccando i concetti di confine e di distanza, lo spazio dell'azione e dell'interazione, separandosi dallo spazio fisico, si è riconfigurato come spazio isolato, immateriale e virtuale, che si colloca al di sopra di qualsiasi altro spazio territoriale[28], innescando quella che il sociologo Zygmunt Bauman definisce «la Grande guerra di indipendenza dallo spazio», ossia una «una guerra durante la quale i centri decisionali, insieme alle motivazioni stesse che determinano le decisioni, gli uni e le altre ormai liberi da legami territoriali, hanno preso a distaccarsi, in forma continua e inesorabile, dai vincoli imposti dai processi di localizzazione»[29]

Una "guerra" – si noti bene – a cui l'Europa prende parte nel tentativo di tornare a riaffermare quella territorialità da cui i luoghi (virtuali del cyberspazio), le informazioni ed il potere sono stati progressivamente svincolati, al fine di riconfigurare quell'ambito costituito dai flussi di informazione che corrono all'interno della rete elettronica come spazio di conquista e controllo, su cui affermare sovranità, confini e potere[30].

La fine della geografia paventata da O'Brian[31], sembra dunque ancora lontana, e la rivendicazione della centralità del territorio nel suo tradizionale significato di area circoscritta entro confini geografici o politici (anziché area aperta e in continua espansione), sembra permettere alle istituzioni europee di recuperare un «àmbito di signoria»[32] in cui poter continuare ad esercitare il ruolo di regolatori e regolamentatori e a salvaguardare l'autonomia e specificità del proprio diritto[33].

---

[28] Cfr., Z. BAUMAN, *Dentro la globalizzazione. Le conseguenze sulle persone*, (trad. it), Roma. Bari, 1999, p. 17.

[29] *Ibidem,* p. 11.

[30] Cfr., F. DOUZET - A. DESFORGES - K. LIMONIER, *Géopolitique du cyberespace: "territoire", frontières et conflits, Collège international des sciences du territoire,* Mars 2014, Paris, Proceedings du 2e colloque international du CIST, pp.173-178, consultabile all'indirizzo web http://www.gis-cist.fr/wpcontent/uploads/2014/02/douzet-desforges-limonier.pdf;

A.-L. SANGUIN, *Fine della geografia o rivincita della geografia? le società umane in un mondo liscio, un mondo «puntuto» o un mondo piatto*, in *Bollettino della società geografica italiana Roma* - Serie XIII, vol. VII, 2014, pp. 445-460, ma spec., p. 457, osserva come il cyberspazio è profondamente anti-spaziale, dal momento che non si può dire dove sia e che non se ne può descrivere forma e dimensioni. Si possono trovare cose, nel cyberspazio, senza sapere dove siano! In un certo modo, la despazializzazione operata da Internet distrugge la chiave del «geocodice» (Akos, 2009). Per converso, questa nuova forma di comunicazione dipende dai legami spaziali nel mondo reale, dalla posizione geografica dei punti di accesso, dalla materialità dei cavi a fibra ottica, dal WiFi – in assenza di cavi e di fili telefonici. Se l'accesso a Internet è di eccellente qualità in un posto, mentre è assente in un altro posto, questa è un'altra prova dell'importanza della posizione e della localizzazione geografiche

[31] R. O'BRIAN, *The End of Geography? The Impact of Technology and Capital Flows*, in *The AMEX Bank Review*, 1990, 17, 5, pp. 2-5.

[32] Definizione che costituisce il significato letterale del termine *territorium*, come la stessa desinenza rivela. Così, T. PERASSI, *Scritti giuridici,* I, Milano, 1958, p. 103, nota 8

[33] D. R. JOHNSON – D.G. POST, *Law and Borders: The Rise of Law in Cyberspace*, in *Stanford Law Review*, vol. 48, n. 5, 1996, p. 1367, ma spec., 1370, più di vent'anni fa già osservavano come «*Cyberspace radically undermines the*

Si aggiunga poi che tutto ciò che è privo di limiti, di linee di demarcazione capaci di tracciare perimetri precisi e definiti del reale, appare non facilmente conoscibile e può generare legittima paura, mentre, all'opposto, la delimitazione attraverso contorni netti e precisi si presta alla conoscenza e pare offrire maggiore sicurezza. Ed è proprio in quest'ottica che sembra infatti muoversi il nuovo regolamento sulla *privacy*, proponendosi di creare – come si precisa al considerando n.7 – quel «clima di fiducia che consentirà lo sviluppo dell'economia digitale in tutto il mercato interno», assicurando ai singoli individui il controllo dei dati personali che li riguardano e garantendo che «la certezza giuridica ed operativa sia rafforzata tanto per le persone fisiche quanto per gli operatori economici e le autorità pubbliche».

Nel cogliere, dunque, l'impossibilità di far rispettare sul web le leggi come tradizionalmente scritte, là ove esse risultino ancorate al solo principio di stabilimento, il legislatore europeo ha voluto individuare un proprio *ambitus* geografico chiaro e certo in cui poter esercitare la propria sovranità in materia di *privacy*. Per poter fare ciò, per riuscire cioè a ristabilire dei confini netti e precisi all'interno dei quali poter esercitare pieni poteri di controllo su tutti i flussi di informazioni che passano nel Vecchio Continente, l'UE ha optato in definitiva per un capovolgimento dei soggetti attori e ha stabilito che a determinare l'applicabilità della legge europea non sia più il luogo in cui è stabilito il titolare del trattamento, ma il luogo in cui risiede, vive e opera l'interessato persona fisica, se fissato sul territorio dell'Unione Europea. I tradizionali confini segnati dalla territorialità, per certi versi, dunque, permangono e a internet sembra essere quasi restituito uno spazio materiale di riferimento, almeno per ciò che concerne la definizione dei criteri per la sua regolazione, là ove si stabilisce espressamente che a rilevare ai fini dell'applicabilità della normativa europea è la presenza sul *territorio* europeo del soggetto interessato al trattamento dei dati personali.

relationship between legally significant (online) phenomena and physical location. The rise of the global com- puter network is destroying the link between geographical location and: (1) the power of local governments to assert control over online behavior; (2) the effects of online behavior on individuals or things; (3) the legitimacy of a local sovereign's efforts to regulate global phenomena; and (4) the ability of physical location to give notice of which sets of rules apply. The Net thus radically subverts the system of rule-making based on borders between physical spaces, at least with respect to the claim that Cyberspace should naturally be governed by territorially defined rule»; M. BETZU, *Regolare internet. La libertà di informazione e di comunicazione nell'era digitale,* Torino, 2012, *passim,* ma spec., p. 27, fa notare come l'attenuazione del vincolo territoriale comporti come conseguenza naturale l'indebolimento della risposta sanzionatoria, il quale costituisce per molti un carattere ontologico del cyberspazio e rappresenta altresì uno dei molteplici aspetti della globalizzazione, intesa come fenomeno di complessa definizione concettuale che ha profondamento trasformato la società del Novecento e le sue istituzioni. L'Autore, sottolinea poi come ogni comunità giuridicamente ordinata abbia invero bisogno di confini e aggiunge che se il cyberspazio, in senso fisico, è un "non luogo", ciò non significa che esso non possa essere invero controllato.

5. Il diritto alla *privacy* tra problematiche globali e nuove frontiere "nazionali". Spunti di riflessione comparata

Come si puntualizza meglio nel considerando n.9, ferma restando la validità degli obbiettivi e dei principi stabiliti dalla precedente direttiva 95/46, il problema che continuava a persistere, e al quale occorreva porre rimedio, era la frammentazione dell'applicazione della protezione dei dati personali nel territorio dell'Unione e la conseguente «incertezza giuridica o la percezione, largamente diffusa nel pubblico, che in particolare le operazioni online comportano rischi per la protezione delle persone fisiche».

Il rafforzamento e la disciplina dettagliata ed uniforme dei diritti degli interessati e degli obblighi di coloro che effettuano e determinano il trattamento dei dati personali per tutti gli Stati membri (ricorrendo allo strumento del regolamento, più adatto, rispetto alla direttiva, ad assicurare un adeguato livello di unificazione normativa)[34] costituisce il primo passo per riuscire a creare un ambito di tutela efficace e soprattutto coerente e ben delimitato di protezione dei dati personali.

L'adozione di una disciplina omogenea come quella offerta dal Regolamento della *privacy* appare infatti funzionale a garantire in tutta l'Unione un elevato livello di tutela dei diritti e delle libertà fondamentali della persona fisica con riguardo al trattamento dei dati personali, tale da consentire attraverso il superamento di quei particolarismi nazionali che non soltanto sono stati la causa di disparità capaci di ostacolare la libera circolazione dei dati personali nel mercato interno europeo, ma hanno anche reso difficile il controllo di un potere tecnocratico di respiro transnazionale che, per sua natura, tende a sfuggire, alla vigilanza dei singoli Stati[35].

I confini territoriali dei singoli Stati sono infatti risultati sempre più inidonei a fungere da efficace baluardo contro le ingerenze nella vita privata del singolo individuo. Essi, da tempo, conoscono «nuove e variegate manifestazioni di irrilevanza»[36] a fronte di un diritto sopranazionale che sembra offrire maggiori garanzie anche in considerazione del riconoscimento di «poteri equivalenti per controllare e assicurare il rispetto delle norme di protezione dei dati personali» e di «sanzioni equivalenti per le violazioni in tutti gli Stati membri» (considerando 11 del regolamento).

---

[34] C. COLAPIETRO, *I principi ispiratori del Regolamento UE 2016/679 sulla protezione dei dati personali e la loro incidenza sul contesto normativo nazionale La tempistica di un simile cambiamento, con il passaggio dallo strumento della Direttiva a quello del Regolamento* in *Federalismi.it,* n. 22/2018, p. 3, fa notare come la scelta di regolare la materia con Regolamento, anziché direttiva non sia certo casuale. Nel pieno dell'era digitale – osserva l'Autore – vi è la diffusa sensazione che i nostri dati personali siano costantemente a rischio e che vi sia una sorta di «costante ipoteca» (l'espressione è di P. PASSAGLIA, *Privacy e nuove tecnologie, un rapporto difficile. Il caso emblematico dei social media, tra regole generali e ricerca di una specificità*, in Consulta Online, III, 2016, p. 334) sulla inviolabilità della propria sfera privata e – soprattutto – sulla controllabilità della circolazione dei propri dati con la conseguenza di ritenere necessario assicurare un'applicazione della disciplina sulla *privacy* omogenea su tutto il territorio dell'Unione europea.

[35] In questo senso, L. CHIEFFI, *La tutela della riservatezza dei dati sensibili: le nuove frontiere europee,* in *Federalismi.it,* n. 4/2018

[36] M.R. FERRARESE, *Diritto sconfinato. Inventiva giuridica e spazi nel mondo globale,* Roma-Bari, 2006, p. 16

Se i territori nazionali vengono progressivamente «privati dei loro recinti, che li mettevano in isolamento, e vengono investiti da circuiti globalizzati»[37], il bisogno – come si è visto – di porre però un argine alla completa deterritorializzazione delle tecnologie e la necessità di riperimetrare uno spazio fisico entro cui saranno applicate le regole che un'istituzione sopranazionale come l'UE approverà, permangono e si fanno sentire ancor di più a causa dell'assenza di una visione di *privacy* e della sua tutela universalmente condivisa.

In tal senso, se, per certi versi, dunque il diritto travalica i confini tradizionali statali aprendosi a nuove dimensioni (come quella internazionale e transnazionale), perché senza limiti spaziali, oltre che temporali, sono i problemi cui l'umana convivenza deve far fronte nel tentativo di rispondere a bisogni, motivazioni, aspirazioni o interessi che appartengono ad ogni individuo, è altresì vero – come è stato osservato[38] – che la globalizzazione non riesce ad intaccare del tutto lo Stato nazionale, seppure ne relativizzi notevolmente la "sovranità" [39], come dimostra il fatto che «la stessa Unione europea, in fondo, punta ad assumere le sembianze dello Stato sovrano e a rivendicare per sé una quota di sovranità».

Siamo d'altra parte ancora distanti dal poter prospettare l'esistenza di una *lex electronica*, chiamata a regolare il ciberspazio, evolutasi – in modo del tutto analogo all'altra più nota manifestazione di diritto transnazionale che è la *lex mercatoria* – prevalentemente in autonomia e capace di stabilire una «costituzione digitale globale»[40]. Come ci ricorda Harold Kohn, *legal adviser* presso il *U.S. Department of State,* gli Stati che svolgono attività nel cyberspazio devono tener conto della sovranità di altri Stati, anche al di fuori del contesto dei conflitti armati. L'infrastruttura fisica che supporta Internet e le attività cibernetiche è generalmente ubicata sul territorio sovrano e soggetta alla giurisdizione dello Stato territoriale. A causa della natura interconnessa e interoperabile del cyberspazio, le operazioni mirate alle infrastrutture informatiche in rete di un Paese possono avere effetti in un altro Paese e, pertanto, «*whenever a State contemplates conducting activities in cyberspace, the sovereignty of other States needs to be considered*»[41].

---

[37] Ancora, M.R. FERRARESE, *op. cit.,* p. 66

[38] In questo senso, R. BIN, *Ordine giuridico e ordine politico nel diritto costituzionale globale.* Relazione svolta al Convegno *Ordine giuridico e ordine politico esperienze, lessico e prospettive,* Trento 24-25 novembre 2006, consultabile, per il quale «Lo Stato resta non solo il paradigma di riferimento ancora insuperato dell'esercizio dei poteri pubblici, ma anche lo strumento su cui appoggia la globalizzazione»

[39] Vedi, sul punto, A. CAMMILERI, *L'euro-cybersécurité à l'ereuves des frontières,* in *La fontière revisitée. Un concept à l'epreuve de la globalisation, Livres de l'Institut Universitaire Varenne/Colloques & Essais,* 2016, pp. 175-190, ma spec., p.181, per la quale «*les frontiéres juridiques internationales de la lutte contro la cybercriminalité passent par l'harmonisation d'un systéme juridique de prévention et de sanctions bien lent à émerger*», il che comporta un «*retour en force du critère de territorialité – donc implicitament des frontières des États – pour sanctionner les auteurs des cyberattaques*».

[40] M.R. FERRARESE, *op. loc. cit.,* cui si rinvia per ulteriori riferimenti bibliografici

[41] Così, H. KOH, *Legal Adviser of the U.S. State Dep't On the speech in relation to Tallinn Manual 1.0*, consultabile in M. N. SCHMITT, *International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed*, *Harvard International Law Journal,* online, vol. 5, 2012, p. 13; M.N. SCHMITT - L. VIHUL, *Respect for Sovereignty in Cyberspace*, in *Texas Law Review,* vol. 95, 2017, p. 1639

Le minacce derivanti dall'impiego di sofisticate tecnologie nel campo dell'informatica richiedono a gran voce l'intervento dei poteri pubblici al fine di assicurare un'effettiva e concreta tutela di quei diritti fondamentali che paiono direttamente connessi al trattamento dei dati personali. Di qui la rivendicazione da parte di un organismo sopranazionale come l'UE del potere di disciplinare – e difendere – il diritto dell'individuo ad autodeterminare il proprio corpo e le informazioni che gli appartengono: un intervento quello europeo reso ancor più necessario per il fatto che, come sopra accennato, il problema non è solo quello di adoperarsi per orientare l'impiego di quelle nuove tecniche di comunicazione e informazione che hanno introdotto profonde trasformazioni e sono foriere allo stesso tempo di nuovi e positivi sviluppi ma anche di rischi per la libertà del singolo. Ciò che sembra emergere è piuttosto la necessità di stabilire regole che assicurino un adeguato livello di tutela dei diritti fondamentali, e nella fattispecie di quello alla privacy, sul territorio europeo, in risposta – come già sopra accennato – alla mancanza di un comune e globale sentire in materia di protezione dei diritti connessi al trattamento dei dati personali.

E' sufficiente il raffronto con gli Stati Uniti per rendersi conto di come le tutele risultino differenti e di quanto appaia allora fondato il timore delle istituzioni europee di non vedere sufficientemente protetta, la vita privata di chi risiede sul proprio territorio.

Recentemente la stessa dottrina statunitense[42] ha evidenziato come in un contesto internazionale ove sembra potersi avvertire una tendenza globale a proteggere in modo più efficace gli individui da illegittime invasioni della *privacy* (ne è una conferma il diffuso riconoscimento ad opera di molti Paesi di un diritto "naturale" alla *privacy*), gli Stati Uniti appaiano invece in ritardo nella protezione dei dati personali dei propri cittadini. Dal raffronto con l'Unione europea, ma anche da quello con alcuni Paesi latino-americani, negli Stati Uniti, a differenza di altri contesti giuridici, si avverte la mancanza di una disciplina organica e omogenea in materia e la presenza al suo posto di una sorta di « "*patchwork quilt" of personal data protection*»[43] fondato su un approccio settoriale creato "a ritroso", ovverosia «*rather than coming up with an*

[42] S. L. LODE, *"You Have The Data"... The Writ Of Habeas Data And Other Data Protection Rights: Is The United States Falling Behind?,* in *Indiana L. Journ. Supplement,* vol. 94, 2018, p.41

[43] *Ibidem,* p. 56 per la quale l'approccio adottato dagli USA nella protezione dei dati sembra piuttosto «*to be one of fixing specific problems in topical areas as they arise*». Ne è un esempio, il *Cable Television Consumer Protection and Competition Act*, che ha modificato il Communications Act del 1934, il quale si occupa di problemi di dati e di protezione dell'informazione dei consumatori in relazione all'afflusso di televisione via cavo negli anni '90, e il Fair Credit Reporting Act fornisce la protezione della *privacy* delle informazioni dei consumatori conservate dalle agenzie che raccolgono le segnalazioni dei consumatori. Questi non sono gli unici casi in cui il Congresso ha perso l'occasione per introdurre una regolamentazione di ampio respiro riguardante i trattamento di dati personali in generale, preferendo adottare singoli provvedimenti normativi, il cui ambito di applicazione è limitato solo a specifiche aree (si pensi ad esempio al *Federal Trade Commission Act*, al *Children's Online Privacy Protection Act*, al *Electronic Communications Privacy Act*, al *Controlling the Assault of Non-Solicited Pornography and Marketing Act* e ancora al *Health Insurance Portability and Accountability Act*). L'Autrice auspica allora che le recenti novità legislative in materia di *privacy* adottate da numerosi ordinamenti stranieri possano fungere da esempio per gli Stati Uniti, che, dal canto loro,

overall picture and then breaking it up into smaller pieces that mesh together» si è preferito da parte del Congresso «*sporadically creating individual pieces of ad hoc legislation*»[44]. In sostanza, negli Stati Uniti manca una normativa equivalente al recente Regolamento della *privacy* e, ancor prima, alla direttiva 95/46CE o assimilabile alla legge federale svizzera sulla protezione dei dati del 19 giugno 1992 (revisionata nel 2014). L'approccio che si rileva è *ad hoc*, vale a dire che ogni legge o regolamento contiene disposizioni in materia di protezione dei dati per ogni settore (in cui sorgano questioni inerenti la protezione della *privacy*) e le disposizioni possono anche essere frutto di una autoregolamentazione, una sorta cioè di *best practice* messa a punto da agenzie governative o gruppi industriali attraverso la codificazione di *guidelines* prive di forza di legge.

Questo mosaico composto da leggi e regolamenti federali e statali che spesso si sovrappongono, incastrano e si contraddicono a vicenda e che restituiscono un quadro normativo complessivamente frammentato e disomogeneo da Stato a Stato si contrappone dunque alla scelta diametralmente opposta dell'Unione europea di adottare un approccio generalista (indipendentemente dal settore di applicazione) e centralizzato, scelta oggi vieppiù rafforzata dall'introduzione del nuovo Regolamento, ossia di una normativa direttamente applicabile, la quale non necessita di una legislazione di attuazione negli Stati membri, con la quale garantire una maggior armonizzazione legislativa nell'Unione. A ciò va poi aggiunta un'altra considerazione non di poco conto: negli Stati Uniti gli utenti delle moderne tecnologie sono tutelati soprattutto in veste di consumatori e la tutela della loro *privacy* è, non a caso, attribuita principalmente alla FTC (*Federale Trade Commerce*) che interviene in materia proteggendo i dati personali come estensione della tutela del consumatore e della legittimità del *fair trade;* numerose sono, infatti, le leggi sulla tutela dei consumatori, che non sono leggi propriamente e specificatamente sulla *privacy*, ma sono normative utilizzate per proibire pratiche sleali o ingannevoli che implicano la divulgazione di informazioni personali.

Se a Warren e Brandeis va certamente il merito di aver affrontato per la prima volta il problema del bilanciamento tra il diritto all'informazione (il diritto ad essere informati) e il diritto alla *privacy*, cioè il diritto alla riservatezza per gli individui, è altresì vero che i successivi sviluppi della normativa statunitense non hanno condotto verosimilmente agli stessi risultati raggiunti nel Vecchio Continente ove si assiste ad un formale riconoscimento del diritto in questione (artt. 7 e 8 della Carta dei diritti fondamentali, oltre a

potrebbero ispirarsi a esperienze giuridiche diverse dalla propria per migliorare la protezione di dati personali, soprattutto di quelli più sensibili, relativi alla salute.

[44] Come si legge in *U.S. dep't of commerce, internet policy task force, commercial data privacy and innovation in the internet economy: a dynamic policy framework, 60 (2010),* http://www.ntia.doc.gov/report/2010/commercial-data-privacy-andinnovation-internet-economy-dynamic-policyframework [https://perma.cc/K9KM-WT5L]

quello previsto in alcune Costituzioni dei Paesi membri[45]) e ad un progressivo e parallelo sviluppo di una ricca normativa *ad hoc*, espressamente indirizzata a regolamentare il trattamento dei dati personali.

Negli Stati Uniti, ove il formante giurisprudenziale riveste un ruolo privilegiato, come vuole un sistema tradizionalmente di *common law,* la Corte Suprema[46] ha contribuito a riconoscere un vero e proprio diritto alla *privacy* da tutelare nella *penumbra* di alcuni diritti del *Bill of Rights* del 1791; ciononostante non si è mai provveduto ad una espressa collocazione e identificazione della *privacy* come situazione giuridica fondamentale in un testo di legge, come è invece avvenuto in Europa, a partire già dalla Convenzione europea dei diritti dell'uomo del 1950 che ha riconosciuto il diritto al rispetto della vita privata di una persona (art. 8, comma 1) a cui segue la Convenzione n.108 del 1981 (c.d. Convenzione di Strasburgo), che reca un'articolata enunciazione di principi a cui dovrebbero (o almeno, avrebbero dovuto) conformarsi le varie legislazioni nazionali, in modo da assicurare il rispetto del diritto alla *privacy* degli individui nei confronti di ogni elaborazione automatizzata di dati concernenti soggetti identificati o identificabili, e infine la più recente Carta di Nizza in cui si sancisce definitivamente l'esistenza di un "diritto alla protezione dei dati di carattere personale" distinto e autonomo dal "diritto alla riservatezza".

Il diverso approccio adottato dai due ordinamenti, europeo e statunitense, non poteva non suscitare legittime preoccupazioni da parte dell'Unione per la sicurezza dei dati personali visto che negli USA non viene garantita secondo standard condivisi o perlomeno assimilabili a quelli adottati nel Vecchio Continente. Lo stesso, più recente accordo Scudo EU-USA per la *privacy* (il *Privacy Shield*), stipulato tra Commissione Europea e Dipartimento del Commercio degli Stati Uniti nel 2016 allo scopo di proteggere la riservatezza dei dati personali dei cittadini europei in caso di trasferimento oltreoceano a scopo commerciale è apparso insufficiente a regolare la realtà digitale. Allo stesso tempo, accanto al "modello" USA di governo dei dati, monopolizzato di fatto da un gruppo ristretto di grandi *private corporations,* se ne sta affermando un secondo, distinto dal primo, ma egualmente capace di generare legittimi timori su possibili rischi in cui possano incorrere i diritti digitali: si tratta del "modello" cinese caratterizzato dal fatto che la rete è subordinata al controllo esclusivo dello Stato e la raccolta dati è concepita come uno strumento da cui trarre significativi vantaggi non solo da un punto di vista economico, ma anche politico,

[45] Si pensi ad esempio alla Spagna e all'art. 18.1 della costituzione; a quella belga e al suo art. 22; agli artt. 26 e 35 della Costituzione portoghese del 1982

[46] Per tutti, si rammenti il caso della *Supreme Court, Griswold v. Connecticut*, 381 U.S. 479, 85 S. Ct. 1678, 14 L. Ed. 2d 510 (1965). Per un commento, cfr., H. T. Greely, *A Footnote to "Penumbra" in Griswold V. Connecticut*, in *Constitutional commentary,* n. 6, 1989, p. 251; G. VIGGIANI, *Il* penumbral reasoning *nella giurisprudenza nordamericana,* in *Jura Gentium,* online, 2017

visto che l'immagazzinamento di informazioni personali da parte del governo di Pechino è concepito dal medesimo come un mezzo per poter sorvegliare in modo massiccio e globale i propri cittadini[47].

L'ascesa della Cina nel campo dell'intelligenza artificiale è d'altra parte avvenuta ad una velocità tale da far sorgere il dubbio che, a breve, le aziende del Sol Levante possano arrivare prima di altre a disporre di programmi informatici talmente avanzati e, allo stesso tempo, così a buon mercato da riuscire ad invadere l'Occidente, conquistandolo "digitalmente"[48].

Nell' interfacciarsi con il governo di Pechino non si può poi dimenticare che ci si sta rapportando con un ordinamento in cui lo sviluppo di un diritto (se di una situazione giuridica fondamentale si voglia e si possa qui parlare) alla *privacy* è avvenuto secondo modalità ben diverse da quelle in cui si è verificato in Europa e negli stessi Stati Uniti, e ciò in ragione della considerevole diversità dei contesti giuridici di riferimento che chiunque si avventuri in uno studio comparato deve tenere necessariamente conto.

Il confronto fra soluzioni normative adottate da ordinamenti così differenti in risposta a problemi pratici più o meno analoghi, creati dagli sviluppi sociali, economici, politici impone quindi una comparazione che rilevi innanzitutto le somiglianze e le diversità presenti nella formulazione semantica stessa delle normative stesse e di specifici istituti[49].

Non solo.

Va sempre tenuto a mente che la *privacy* rappresenta un concetto elaborato in Occidente e circolato a livello globale; non tutte le frontiere sono però così porose come si pensa, e pertanto occorre verificare se e quanto la *privacy*, trapiantata in Cina, funzioni effettivamente allo stesso modo in cui opera in Europa e negli USA, visto che ci troviamo dinnanzi a strutture socio-economiche e politiche ampiamente

---

[47] J. D. FRY, *Privacy, predictability and internet surveillance in the U.S. and China: better the devil you know?* in U. Pa. J. Int'l L. vol. 37, 419, 2015; J.-A. LEE, *Hacking into China's Cybersecurity Law*, in *Wake Forest Law Review*, vol.53, 2018; Z. WANGL, *Systematic government access to private-sector data in China*, in *International Data Privacy Law*, vol. 2, n. 4, 2012, p. 220, il quale osserva: «*the government's systematic access to data held by anyone will become possible and realistic with the evolution of the e-government strategy, in accordance with its vital interest of maintaining the state's control on information and "'preserving the stability' of the society* » (p. 222)

[48] Sebbene il paese asiatico abbia approvato un'interessante normativa per la tutela dei dati personali già nel 2012 ci sono ancora numerose ragioni per nutrire preoccupazioni in merito alla gestione dei dati. Oltre, infatti, ai ragionevoli timori dovuti alla natura autoritaria del governo, nella Repubblica Popolare Cinese la cosiddetta *Cybersecurity Law* obbliga tutte le aziende a conservare i dati in server ubicati sul territorio cinese e, laddove richiesti, a fornire al governo le chiavi di decriptazione, il codice sorgente dei software e qualsiasi altra informazione che le pubbliche autorità possano ritenere rilevante. La conseguenza è che manca una netta divisione tra i dati posseduti dalle società e quelli di proprietà del governo, informazioni che, al contrario, si incrociano e intrecciano fra loro, conducendo ad un'unica, estrema profilazione (*rectius,* un totale e pervasivo controllo) dei cittadini-utenti.

[49] T. LI-Z. ZHOU - J. BRONFMAN, *Saving face: unfolding the screen of chinese privacy law* in *Journal of law, information and science, (Forthcoming),* consultabile all'indirizzo web https://ssrn.com/abstract=2826087, raccomandano di non affrontare lo studio della normativa cinese sulla *privacy* «*in a vacuum*», sottolineando come « *to understand Chinese privacy law, we must juxtapose Western notions of privacy against thousands of years of Confucian teaching and the historical background of communism that still influences present-day Chinese society*»

divergenti fra loro[50], le quali inevitabilmente hanno condizionato e condizioneranno ulteriormente il sistema di protezione dati all'interno del singolo sistema giuridico di riferimento[51].

D'altra parte, come si è già osservato, anche in un ambito più omogeneo, come quello occidentale, il confronto fra Europa e Stati Uniti fa comunque emergere più differenze che analogie nella gestione della *privacy*, una distanza che spiega la necessità da parte dell'UE di approntare maggiori tutele ai propri consumatori, i cui dati personali siano elaborati e trattati dai colossi della *Silicon Valley*.

E' chiaro allora che in uno simile contesto caratterizzato dalla presenza di due potenze industriali che si contestano la supremazia tecnologica e rivendicano – attraverso anche i propri *big-tech* – la propria egemonia nel campo del controllo dei dati scambiati da una parte all'altra nel mondo, i rischi per la *privacy* sono alti e il bisogno di ristabilire lo Stato di diritto nel cyberspazio diviene una priorità irrinunciabile. L'Europa, meno competitiva sul fronte dello sviluppo digitale, ha, così, optato per un approccio diverso da quello adottato dagli USA e dalla Cina, basato sostanzialmente sulla protezione dei nuovi diritti digitali emersi negli ultimi anni nella società contemporanea, come conferma l'entrata in vigore del regolamento GDPR a difesa della *privacy* personale, contro le minacce provenienti dalle pratiche disinvolte dei giganti del web, e la proposta di direttiva, recentemente approvata dal Parlamento europeo (il 26 marzo 2019) sulla protezione del diritto d'autore nel mercato unico digitale, resa necessaria dall'evoluzione delle tecnologie digitali che ha cambiato anche il modo in cui le opere e altro materiale protetto vengono creati, prodotti, distribuiti.

La necessità di regolamentare il mondo del web avvertita dall'Unione europea rappresenta il tentativo delle sue istituzioni di fronteggiare l'avanzata di quel "capitalismo della sorveglianza" che come sopra

---

[50] Cfr., in generale, sul problema della circolazione e trasmissibilità del diritto straniero, C. PINELLI, *Trapianti, innesti, dialoghi. Modalità di trasmissione e circolazione del diritto straniero,* in *Rivista trimestrale di diritto pubblico,* in *Rivista trimestrale di diritto pubblico,* n.2, 2011, p. 495

[5151] Cfr., sul punto, C. JINGCHUN, *Protecting the right to privacy in China*, in *Victoria University of Wellington Law Review* vol. 36, n. 3, 2005, p.645, che precisa come *«the modern concept of privacy has been absorbed by Chinese scholars and defined according to Chinese norms»* e come *«The right to privacy has been recognised as one of the most fundamental human rights worldwide»* e pur tuttavia *«the development of legal protection of privacy in mainland China is at least 10 years behind that of Western countries».* W. LIMING, *The Redefinition of the Concept of the Right to Privacy*, in *The Jurist,* 2012, pp. 108–111, ha cura di sottolineare come la *privacy* non appartenga alla tradizione culturale cinese, trattandosi di un istituto importato dall'Occidente, evidenzia come le differenze fra il modello cinese di tutela della vita privata e quello occidentale «*are more than just legal*». Il concetto cinese si contraddistinguerebbe infatti per "*the purpose of promoting social harmony, and, therefore, this is very different from the western system, which is based on human rights and freedoms*". A ciò si aggiunga poi la considerazione per cui in Cina «*the personality right, such as privacy, should be purely a civil law right, unlike in the Europe and US where privacy has a constitutional dimension*». La Cina, osserva C. LEI, *Debating Personality Rights Protection in China: A Comparative Outlook*, in *European Review of Private Law,* n. 1, 2018, pp. 31-56, non possiede «*a Human Rights Law, or a constitutional court. Therefore, there is an urgent need to grant protection to personality rights by entrenching them in the private law sphere through their inclusion in the future Chinese Civil Code*. Cfr., altresì, C. JINGCHUN, P*rotecting the right to privacy in China*, in *Victoria University of Wellington Law Review,* n. 36, 2005, p. 645

accennato è sempre più radicato nelle odierne società e che sempre più spesso viene a stringere una sorta di alleanza con il controllo esercitato dallo Stato– come nel caso della Cina, della Russia e in parte anche degli USA – unendo insieme l'interesse dello Stato con quello imprenditoriale e dando origine ad un pericoloso sodalizio fra poteri pubblici e poteri privati invero già avvezzi - ma ora ancor più – ad agire senza limiti.

6. La protezione dei dati viaggia con i dati: la disciplina dei trasferimenti di dati personali fuori UE

Come è stato osservato[52], l'immaterialità e l'intrinseco legame con le reti di telecomunicazione che contraddistinguono i dati (digitali) non consentono ai medesimi di radicarsi in modo netto e preciso nel territorio e nel sistema giuridico di un solo Stato: una volta acquisiti dalle tecnologie c.d. *cloud*, le informazioni vengono infatti utilizzate, trasferite, elaborate, cedute, duplicate numerose volte, e quando vengono restituite non corrispondono quasi più a quelle depositate, rendendo così più difficile stabilire a chi esse realmente appartengano, se a coloro che le generano o, piuttosto, a coloro che le raccolgono e le elaborano[53].

Se però la liquidità del mondo digitale e la circolazione/rielaborazione dei dati rischiano di rendere vane le pretese giuridiche del titolare di esercitare appieno il proprio diritto domenicale sulle informazioni che lo riguardano, il controllo pubblico sull'uso che terzi possono fare di tali dati è invece possibile ed anzi auspicabile, come dimostra, ad esempio, l'impiego che in questi anni è stato fatto di autorità amministrative indipendenti (a livello nazionale ed europeo) preposte a sorvegliare sul rispetto del diritto alla vita privata e sulla protezione dei dati in sede di trattamento dei dati personali e di elaborazione di nuove politiche, e come conferma naturalmente il nuovo GDPR che oltre a potenziare il ruolo dei Garanti, stabilisce regole più chiare in materia di informativa e consenso, definisce i limiti al trattamento automatizzato dei dati personali e stabilisce criteri e sanzioni rigorosi nel caso in caso di violazione delle informazioni raccolte.

L'Europa, come si è già osservato, ha manifestato con la nuova normativa la volontà di (ri-) affermare la propria sovranità in materia di raccolta, utilizzo e circolazione di dati personali, e nel dare seguito a questo suo proposito, ha voluto regolare anche l'ipotesi di trasferimento di dati verso Paesi terzi o organizzazioni internazionali reso necessario o quanto meno inevitabile dall'espansione del commercio internazionale e dalla cooperazione sovranazionale

[52] V. ZENO-ZENCOVICH, Dati, grandi dati, dati granulari e la nuova epistemologia del giurista, in *Rivista di diritto dei media,* 2/2018, p. 1

[53] E. PROSPERETTI, *L'opera digitale tra regole e mercato,* Torino, *passim,* ma spec., p. 262

Come si rammenta nel quinto considerando del regolamento, l'integrazione economica e sociale conseguente al funzionamento del mercato interno ha condotto a un considerevole aumento dei flussi transfrontalieri di dati personali e quindi anche dei dati personali scambiati, in tutta l'Unione, tra attori pubblici e privati, comprese persone fisiche, associazioni e imprese, e la rapidità dell'evoluzione tecnologica assieme alla globalizzazione hanno influito significativamente sulla portata della condivisione e della raccolta di informazioni personali, facilitando il trasferimento di quest'ultime verso Paesi terzi ed organizzazioni internazionali, e rendendo quanto mai necessario garantire la definizione di un quadro normativo solido e coerente di tutela.

Il regolamento, ribadisce quanto già in parte stabilito dall'art. 25, primo comma, della direttiva 95/46/CE, optando per una disciplina che fondi la circolazione delle informazioni personali su una decisione di adeguatezza anziché su un astratto principio di equivalenza normativa: l'approccio funzionale scelto dalla normativa europea esclude cioè qualsiasi valutazione aprioristica, dando piuttosto rilievo all'effettività della situazione esistente nell'ordinamento dello Stato terzo complessivamente considerato.

Ad integrazione di quanto precedentemente stabilito dalla direttiva summenzionata, il regolamento individua, nella fattispecie, il soggetto competente a valutare l'adeguatezza del livello di protezione riscontrabile nello Stato terzo, piuttosto che lasciarne l'identificazione alla discrezionalità degli Stati membri. Secondo l'art.45, è infatti la Commissione a decidere, con effetto sull'intera Unione, se un Paese terzo, o un territorio o un settore specifico all'interno di un Paese terzo, o un'organizzazione internazionale siano in grado di offrire un livello adeguato di protezione dei dati e se i trasferimenti di dati potranno avvenire senza che siano richieste ulteriori autorizzazioni.

Non solo.

Diversamente dalla direttiva del 1995 che non definiva in cosa consistesse l' "adeguatezza", né precisava quali fossero le condizioni che consentivano in concreto di ritenerla verificata, il regolamento, già nel considerando 104 e poi nel successivo secondo comma dell'art. 45, precisa i parametri su cui deve incentrarsi la valutazione della Commissione. Ciò che, ancora una volta, spiega la scelta non casuale di regolare il trattamento dei dati personali attraverso una fonte derivata avente portata generale, obbligatoria in tutti i suoi elementi e direttamente applicabile negli ordinamenti degli Stati membri, anziché con una direttiva, rivolta esclusivamente ai Paesi facenti parte dell'UE (e non anche a persone fisiche o giuridiche) che rischia di non garantire un uniforme e soprattutto efficace livello di tutela della *privacy* nell'intera Unione.

Con il regolamento, il legislatore europeo sottrae alla scelta discrezionale dei singoli Stati membri l'individuazione dei valori fondamentali che occorre tener conto per stabilire l'adeguatezza di un Paese terzo, e fissa perentoriamente i valori che devono essere rispettati per poter superare l'esame della

Commissione: stato di diritto, accesso alla giustizia, norme e standard internazionali in materia di diritti dell'uomo, legislazione generale e settoriale riguardante segnatamente la sicurezza pubblica, la difesa e la sicurezza nazionale, come pure ordine pubblico e diritto penale sono i criteri che permettono di testare la reale capacità di uno Stato di riuscire a garantire un adeguato livello di protezione dei dati sostanzialmente equivalente a quello assicurato all'interno dell'Unione; a ciò vanno poi aggiunti, come ulteriori elementi indispensabili ai fini del riconoscimento dell'adeguatezza, la presenza di autorità di controllo indipendenti, competenti a sorvegliare il rispetto delle norme in materia di protezione dei dati e capaci di interloquire e cooperare con istituzione analoghe, presenti sul territorio europeo, e la previsione di diritti effettivi e azionabili oltre ad un mezzo di ricorso effettivo in sede amministrativa e giudiziale.

Nel focalizzare l'attenzione sul possibile aumento di rischi derivanti dai trasferimenti transfrontalieri di dati personali al di fuori dell'UE, che potrebbero compromettere la capacità della persona fisica di esercitare il proprio diritto alla *privacy* e tutelarsi contro usi e comunicazioni illecite di informazioni che la riguardano, la normativa in esame permette alla Commissione di mettere in discussione in qualsiasi momento l'idoneità di uno Stato terzo a garantire un livello adeguato di protezione delle informazioni personali, imponendo a tutte le aziende anche straniere che hanno a che fare con gli «interessati che si trovano nell'Unione» (considerando n. 24) di adeguare la propria *privacy policy* al Regolamento Europeo, se vorranno continuare a operare all'interno dell'Ue.

7. Spunti conclusivi

La rivendicazione di una sovranità "europea" nel trattamento dei dati personali riflette la necessità da parte del Vecchio Continente di gestire in modo autonomo il complesso bilanciamento *privacy*-sicurezza che oggi, come ci mostra il Regolamento 2016/679, non si fonda più solo sulla necessità di contemperare due opposte esigenze, la sicurezza della collettività e la *privacy* del singolo, ma va letto anche in una chiave diversa, capace di mettere in luce il rapporto di affinità (anziché di contraddizione) tra la sicurezza "individuale" dei propri dati, intesa come naturale declinazione del concetto di autodeterminazione informativa, e il diritto alla riservatezza delle informazioni. D'altra parte, la circostanza per cui la protezione dei dati costituisca ormai un baluardo contro illeciti controlli che incidono sulla nostra libertà, evidenzia come, a sua volta, la tutela della *privacy* non sia solo un diritto individuale, ma assurga altresì ad interesse generale fondamentale dello Stato.

Il quarto considerando del Regolamento europeo sottolinea, infatti, come il trattamento dei dati personali debba essere al servizio dell'uomo ed il diritto alla protezione delle informazioni di carattere personale vada considerato alla luce della sua funzione sociale, anziché come una prerogativa assoluta.

In un tempo allora in cui si rivendica a gran voce la sicurezza degli Stati, in nome della quale si adottano (o si promettono di adottare) politiche nazionali di controllo sempre più stringenti e si studiano misure volte a difendere i confini nazionali, anche la *privacy*, intesa come presidio irrinunciabile di tutte le libertà e allo stesso tempo come interesse generale della società, merita alcune riflessioni sull'adeguatezza della normative esistenti a difendere la dimensione individuale della sicurezza (intesa come sicurezza dei dati), garantendo la presenza di quel clima di fiducia atto a consentire lo sviluppo dell'economia digitale in tutto il mercato interno.

Come ci ricorda, infatti, il regolamento, è più mai indispensabile che «le persone fisiche abbiano il controllo dei dai personali che li riguardano e che la certezza giuridica e operativa sia rafforzata tanto per le persone fisiche quanto per gli operatori economici e le autorità pubbliche» (settimo considerando); solo così è possibile contribuire alla realizzazione di uno spazio «di libertà, sicurezza e giustizia e di un'unione economica, al progresso economico e sociale, al rafforzamento e alla convergenza delle economie nel mercato interno e al benessere delle persone fisiche».

L'antica dicotomia *privacy*/sicurezza sembra lasciare dunque il posto a un più complesso rapporto di complementarità in cui l'una e l'altra appaiono muoversi verso una medesima direzione che li vede affermarsi non solo come "diritti individuali", ma anche come garanzia per gli altri diritti, nella misura in cui la protezione dei dati personali è divenuta nella società attuale sempre più il «presidio irrinunciabile di tutte le libertà classiche delle nostre Costituzioni e, in ultima analisi, della nostra società democratica»[54] e la sicurezza torna a rivendicare il significato di «coscienza della libertà garantita»[55].

La prospettiva individuale della sicurezza che emerge con riferimento ai dati personali appare infatti riconducibile alla previsione di una serie di libertà tradizionalmente connesse alla tutela di una sfera intangibile della persona (sicurezza da), nei confronti non solo delle possibili incisioni da parte di terzi, ma anche dell'arbitrio dei pubblici poteri[56]. Alla tradizionale dimensione collettiva della sicurezza che travalica i confini della persona, per estendersi fino a ricomprendere esigenze collettive, viene dunque ad

[54] Così, F. PIZZETTI, *Privacy e diritto europeo alla protezione dei dati personali, vol. I. Dalla direttiva 95/46 al nuovo Regolamento europeo*, Torino, 2016, p. 10

[55] Così, E. DENNINGER, *Diritti dell'uomo e Legge Fondamentale*, Torino, 1998, p. 94 là ove l'Autore denuncia i rischi di una sicurezza che da promozione inclusiva e garanzia del soddisfacimento, effettivo e sostanziale, dei diritti si declini sempre più in termini «di un'attività statale e in via di principio illimitata per tutelare il cittadino da rischi e pericoli sociali causati dalla tecnica o dall'ambiente o anche dal crimine». Un passaggio, quello dalla «sicurezza dei diritti» ad un «diritto alla sicurezza», che condurrebbe ad una riconfigurazione di senso e significato della politica costituzionale dei diritti. Vedi, altresì, G. BASCHERINI, *L'emergenza e i diritti. Un'ipotesi di lettura,* in *Rivista di diritto costituzionale,* 1/2003, p. 3

[56] Vedi, T. GIUPPONI, *La sicurezza e le sue "dimensioni" costituzionali,* in S. VIDA (a cura di), *Diritti umani. Teorie, analisi, applicazioni*, Bologna, 2008, p. 275 (anche in www.forumcostituzionale.it); M. OROFINO, *Diritto alla protezione dei dati personali e sicurezza: osservazioni critiche su una presunta contrapposizione*, in *Rivista di diritto dei media,* 2/2018, p. 1

affiancarsene una seconda, individuale, funzionale alla *privacy* della singola persona, che lungi dal porsi come alternativa alla prima viene piuttosto a compenetrarla e integrarla, a conferma del fatto che la protezione dei dati oggi non sia solo un diritto individuale, ma si configuri ormai anche come un interesse primario della società.

Su queste premesse, si spiega allora la particolare attenzione che il Regolamento europeo ha prestato al trattamento dei dati personali e ai casi di violazione della sicurezza dei medesimi da rinvenirsi non solo nel caso di un evento doloso, come un attacco informatico, ma secondo l'art. 4 del GDPR anche nelle ipotesi di distruzione accidentale o illecita, perdita, modifica, rivelazione non autorizzata o accesso ai dati personali trasmessi, memorizzati altrimenti elaborati. Il nuovo regolamento generale europeo prescrive in particolare specifici adempimenti nel caso in cui si violino dati personali e prevede rilevanti sanzioni di natura amministrativa a conferma della acquisita consapevolezza che la tutela dei dati costituisca ormai uno strumento fondamentale e irrinunciabile non soltanto per la tutela dei diritti ma, più ampiamente, per la tenuta stessa degli ordinamenti democratici.

Il movimento circolare che lega la tutela dei dati alla democrazia e, al contempo, il rischio di espropriazione del diritto da parte della tecnica impongono però necessariamente la definizione di confini che delimitino ciò che può essere considerato "tecnicamente" possibile e ciò che non può, sulla base di soglie di accettabilità da un punto di vista etico e giuridico. E di questo l'Unione europea è apparsa consapevole, vista la decisione di affermare, anche nella dimensione digitale, la propria sovranità attraverso una normativa con la quale ristabilire antichi spazi "scompaginati" dalla rete, entro i quali poter garantire appieno i diritti della persona rispetto a chiunque ne gestisca, con i suoi dati, l'identità.

Nel rivendicare un territorio sovrano, a fronte della riorganizzazione del mondo secondo forme spaziali diverse (liquide e delocalizzate), come quelle offerte dai media, dal telefono o dalla rete di internet, le istituzioni europee hanno voluto rivendicare il diritto di stabilire in pieno autonomia limiti di tutela della *privacy* da considerarsi invalicabili.

Non solo.

Il regolamento europeo nel disciplinare scrupolosamente la materia del trattamento dei dati permette all'Europa di ristabilire quel complesso e difficile rapporto fra sicurezza e *privacy*, sovente letto in senso ostativo anziché di un equo contemperamento realizzato sulla base di un criterio di proporzionalità che rifiuta il controllo "ubiquitario" sul cittadino e propende piuttosto per una lettura basata sul presupposto che le esigenze di sicurezza collettiva non si soddisfano con la generica compressione della *privacy* dei cittadini, ma al contrario con il suo rafforzamento.

Sulla base di questi presupposti, la nuova normativa europea intende offrire un proprio modello di tutela dei dati basato su un'idea di libertà ed una concezione di *privacy* da affermare anche oltre i confini

territoriali superati dalla rete, in contrapposizione non soltanto alla rappresentazione giuridica differente offerta dagli USA, percepita in concreto come attenuata a causa dell'assenza di un modello normativo unico come riferimento al quale aderire, ma anche e a *fortiori* rispetto a forme di sovranità cibernetica – *in primis* quella cinese – che si configurano più come rivendicazioni nazionalistico-autarchiche ed egemoniche che autentiche espressioni di volontà di tutela della *privacy*. Come ci ricorda il nostra Garante per la *privacy*, se prive di regole, le nuove tecnologie rischiano di alimentare un regime della sorveglianza tale «da rendere l'uomo una non-persona, l'individuo da addestrare o classificare, normalizzare o escludere»[57]

Di fronte dunque al sempre più pervasivo utilizzo della tecnologia nella vita privata e pubblica, l'Unione europea appare voler ri-affermare la propria sovranità digitale, senza esigere il riconoscimento di una supremazia nazionale, ma semplicemente rafforzando, entro confini territoriali ben precisi, una propria nozione di *privacy*, nella piena consapevolezza che la presenza di punti di contatto in materia fra distinti ordinamenti (nella fattispecie quello statunitense e quello europeo) non consente invero di parlare di un vero e proprio trapianto giuridico del *right to be let alone* nordamericano in Europa, ma piuttosto di evoluzioni parzialmente parallele che mescolano problemi comuni a strutture istituzionali differenti[58].

L'adozione di un regolamento che si applica non solo alle aziende del Vecchio Continente, ma a tutte le organizzazioni che a vario titolo e indipendentemente dalla loro collocazione geografica conservano informazioni relative ai propri clienti europei consente all'Europa di poter innanzitutto tutelare i propri consumatori sulla base di una propria concezione di *privacy*, non necessariamente condivisa da altri ordinamenti, fondata sul riconoscimento della medesima come diritto fondamentale dell'individuo. Non va poi sottovalutata la funzione che propri, autonomi, standard di protezione dei dati personali potrebbe inoltre svolgere anche nella riduzione dello svantaggio competitivo che si è venuto a creare fra l'Europa e i Paesi tecnologicamente avanzati, primo fra i quali la Cina che oggi vanta una vera e propria leadership nelle reti 5G offerte dal governo di Pechino al resto del mondo.

---

[57] A. SORO, *I confini del digitale. Nuovi scenari per la protezione dei dati,* intervento del Presidente dell'Autorità Garante per la *privacy* alla Giornata europea della protezione dei dati personali, 29 gennaio, 2019, Roma. Il testo integrale è consultabile sul sito www.garanteprivacy.it

[58] J. WHITMAN, *The Two Western Cultures of Privacy : Dignity v. Liberty*, in *The Yale Law Journal*, vol. 113, n.6, 2004, p. 1151 già nel 2004 parlava di incomprensione reciproca fra Stati Uniti ed Europa in merito alla tutela della *privacy*: una sorta di "false friends", una trappola per i comparatisti che hanno sempre creduto erroneamente che i due concetti coincidano, dovendosi invece cogliere delle «*unmistakable differences in sensibilities about what ought to be kept "private"*» (p. 1155); nel comparare più specificatamente la *privacy* statunitense con la *vie privée* francese, J.-L. HALPÉRIN, *Protection de la vie privée et privacy : deux traditions juridiques différentes ?*, in *Les Nouveaux Cahiers du Conseil constitutionnel*, vol. 48, n. 3, 2015, pp. 59-68 rammenta come «*de la persistance d'une expression dans le langage juridique d'un pays, il faut prendre garde de ne pas croire à l'essence de concepts ou de traditions qui seraient le propre d'une culture juridique nationale*» (p. 68).

La rivendicazione di spazi digitali sovrani da parte dell'Europa e l'applicazione del GDPR alla Cina permettono infatti lo sviluppo di una competizione economica nell'ambito della tecnologia informatica e delle comunicazioni il più possibile democratica, governata e trasparente, perché solo proteggendo i nostri dati personali, saremo anche in grado di tutelare il mercato europeo.