MIMMA ROSPI
Dottore di ricerca in Giustizia costituzionale e diritti fondamentali - Università di Pisa
mimmarospi02@gmail.com

LA *DIGITAL TRANSFORMATION* E L'ESERCIZIO DI DIRITTI FONDAMENTALI E DELLE LIBERTÀ PERSONALI: COMPRESSIONE O MIGLIORAMENTO?

DIGITAL TRASFORMATION AND THE EXERCISE OF FUNDAMENTAL RIGHTS AND PERSONAL FREEDOMS: COMPRESSION OR IMPROVEMENT?

SINTESI

L'avvento della tecnologia è paragonabile al periodo della ricostruzione del periodo post-bellico, per forza di cambiamento epocale e ricadute sulla socialità del singolo, nell'esercizio dei diritti fondamentali e delle libertà personali, nonché nei rapporti tra cittadino e Stato.
Gli ultimi eventi causati dalla crisi pandemica hanno accelerato il processo di consapevolezza del fenomeno epocale: la tecnologia è direttamente strumentale allo sviluppo dei popoli. Con questo contributo si intende analizzare il fenomeno dell'utilizzo delle nuove tecnologie come facilitatori dell'esercizio dei diritti e delle libertà fondamentali, verificando se le attuali discipline in tema di neutralità della rete, identità digitali ed *e-government* sono confacenti ai tempi che stiamo vivendo. In particolare, si analizzeranno gli interventi messi in campo dalle istituzioni eurounitarie per realizzare un sistema unionale digitale. Inoltre si analizzerà il caso italiano per verificare l'andamento del miglioramento tecnologico dell'amministrazione digitale al servizio dei diritti e delle libertà fondamentali.

ABSTRACT

The advent of technology is comparable to the period of reconstruction of the post-war period, due to epochal change and the repercussions on the sociality of the individual in the exercise of fundamental rights and personal freedoms, as well as in relations between citizen and State. The latest events caused by the pandemic crisis have accelerated the process of awareness of the epochal phenomenon: technology is directly instrumental to the development of peoples. This contribution aims to examine the phenomenon of the use of new technologies as facilitators in the exercise of fundamental rights and freedoms, assessing whether current disciplines in terms of net neutrality, digital identities and e-government are suited to the times through which we are living. It will examine the measures implemented by the European Union institutions to create a Digital Union Market. In addition, the Italian case will be analysed to verify the progress of the technological improvement of digital administration at the service of fundamental rights and freedoms.

PAROLE CHIAVE: *digital transformation* - *Data governance* - Identità digitali - Amministrazione digitale - Pandemia Covid-19
KEYWORDS: Digital transformation - Data governance - Digital Identity - E-procurement - Covid-19 Pandemic

1. Introduzione

L'avvento della tecnologia ha scardinato i punti fissi del sistema di Stato di diritto costituzionale e democratico, così come era stato delineato non solo nei libri di testo, bensì nella vita concreta e quotidiana di ogni ordinamento giuridico. L'avvento della tecnologia nella vita di relazione degli individui e nelle stanze del potere organizzativo degli Stati, è paragonabile al periodo della ricostruzione post seconda guerra mondiale, per forza di cambiamento epocale e ricadute sulla socialità del singolo, nell'esercizio dei diritti fondamentali e delle libertà personali, nonché nei rapporti tra cittadino e Stato.

La svolta epocale causata dal rapporto tra tecnologia e diritto è stata, tuttavia, a lungo rilegata ad argomento di riflessione minore e, a tratti poco rilevante, per l'analisi dello sviluppo dei tempi e per lo studio del diritto pubblico. L'interesse degli operatori del diritto, e dunque anche dei decisori pubblici, è sorto maggiormente solo dopo che è stato dimostrata dai maggiori *players* delle *new technologies*, la potenza economica e decisionale che l'uso delle tecnologie, *rectius* dei dati, è in grado di innescare sul piano decisionale politico e degli andamenti dei mercati. Gli Stati dunque hanno iniziato ad interessarsi delle ricadute dell'utilizzo delle nuove tecnologie sulle attività di *policy making* e sull'esercizio dei diritti fondamentali.

Mentre le istituzioni pubbliche si sono concentrate prettamente sulle riflessioni in tema di *cybersecurity* e tutela della privacy, in parallelo le multinazionali del mondo digitale sono state in grado di rendersi facilitatori dell'esercizio di molte delle libertà personali e dei diritti del singolo, proprio attraverso l'utilizzo repentino delle tecniche di *data Governance*. In questo modo il cittadino sarebbe stato ben disposto a rinunciare (a volte inconsapevolmente) alle sue tutele, se questo avesse permesso un migliore accesso al web e a tutti i servizi in esso contenuti.

Le istituzioni pubbliche, in ritardo, stanno comprendendo il fenomeno, spostando il baricentro di riflessione anche sulle tematiche della *data Governance* e sulla necessità di imprimere regolamentazioni al riguardo, in specie sul tema delle identità digitali e sull'esercizio dei diritti e delle libertà personali del singolo.

Gli ultimi eventi causati dalla crisi pandemica per la diffusione del Covid-19 hanno avuto, quanto meno, il merito di aver accelerato il processo di consapevolezza del fenomeno epocale: la tecnologia è direttamente strumentare allo sviluppo dei popoli[1]. Con questo contributo si intende analizzare il fenomeno dell'utilizzo delle nuove tecnologie come facilitatori dell'esercizio delle libertà fondamentali, verificando se le attuali discipline in tema di neutralità della rete, identità digitali ed *e-government* sono confacenti ai tempi che stiamo vivendo.

2. Nuove tecnologie, *data governance* e il ruolo dei *players* del digitale

L'avvento di Internet ha portato con sé un nuovo modo di concepire il quotidiano, agevolando le comunicazioni tra soggetti, aumentando le fonti e i contenuti di informazione, in modo sempre più rapido, nonché introducendo una nuova forma di esercizio dei propri diritti e delle proprie libertà.

Il web sembra reggersi su una economia neoliberista in base alla quale è interesse delle multinazionali digitali aumentare (e non ridurre) l'accesso degli utenti. Ciò si apprezza verificando il coinvolgimento in termini di investimenti economici delle grandi multinazionali del digitale sullo sviluppo delle infrastrutture informatiche, e sulla diffusione capillare delle dotazioni ad essi strumentali tra la popolazione. La ragione consiste nella modulazione dei sistemi economici della *e-commerce* e del sistema di *sharing*, per cui i profitti economici in rete, che hanno pervaso tutti i sistemi produttivi e di mercato, "affidano" all'*user* un'attività di condivisione di dati di ogni genere (idee, foto, video, notizie), sulla cui condivisione autonoma del singolo utente si ricava profitto. Infatti i sistemi di *data mining* e di profilazione dell'utente, pongono le aziende digitali innanzi alla necessità di creare quanto più modalità espressive del singolo *user*, per ricavare dalla sua navigazione e dalla sua partecipazione alle piattaforme digitali, come *forum*, *social network* e *communities*, idee, opinioni, interessi, che hanno un elevato valore commerciale, che saranno poi oggetto di una transazione economica[2].

Come acutamente osservato, dunque, «*se da un lato ogni consumatore è incoraggiato a sviluppare la propria personalità in modo autonomo, al tempo stesso questa personalità viene integrata nei fattori di produzione e nella elaborazione delle strategie di commercializzazione*». Si apprezza quanto già era stato rilevato più di un decennio fa, nel ritenere «*come i dati, le informazioni abbiamo preso il sopravvento nelle società contemporanee diventando il bene di maggiore valore, strategico ed economico e mettendo in ombra la libertà di manifestazione del pensiero, o meglio, precisandone i contenuti*»[3]. Di conseguenza

[1] G. TROPEA, *Recensione a S. ZUBOFF, Il Capitalismo della Sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri, Roma, Luiss University Press, 2019 (con una postilla su privacy e covid-19)*, in *Rivista PA, Persona e Amministrazione*, 2020, 1, pp. 479-491.

[2] In tal senso è stato rilevato per uno studio empirico in Inghilterra, C. BENEDIKT FREY, M. A. OSBORN, *The future of employment: how Susceptible are jobs to Computerisation?*, www.oxfordmartin.ox.ac.uk.

[3] V. ZENO-ZENCOVICH, *La libertà d'espressione. Media, mercato, potere nella società dell'informazione*, op. cit., p. 143. In tal senso M. CUNIBERTI, *Tecnologie digitali e libertà politiche*,

la logica economica che governa Internet, è quella di rendere sempre più possibili in termini quantitativi e qualitativi l'utilizzo da parte della popolazione mondiale della rete[4]. Non a caso i *players* più famosi lavorano ormai da anni ad una campagna di finanziamento per esportare il Wi-Fi libero anche nei territori africani.

L'interesse dei giganti di Internet di migliorare l'accesso alla rete da parte dei più si riscontra anche nel loro coinvolgimento da parte di autorità pubbliche nazionali e internazionali nelle attività di politiche che favoriscano l'uso capillare della rete e la riduzione delle problematiche connesse al *digital divide* in senso materiale. È quanto è avvenuto durante il G8 di Okinawa, tenutosi nel luglio del 2000, durante il quale è stato presentato un rapporto dalla *Digital Bridges Task Force*, la cui struttura è stata fortemente caldeggiata dalla GBDE (*The Global Business Dialogue on Electronic Commerce*), la più grande *lobby* della imprenditoria in Internet, con lo scopo di promuovere in tutto il mondo l'*e-commerce* e ridurre le limitazioni fattuali allo sviluppo del commercio elettronico. In questo rapporto è emersa l'importanza della direzione che si deve imprimere alle ICTs, ovvero verso una crescita economica che aumenti il benessere pubblico e la coesione sociale attraverso un accesso libero e ampio alla società d'informazione digitale. Nella *Task force* le *lobbies* di Internet affermano chiaramente che per poter raggiungere questi obiettivi (si ricordi di espansione del *e-commerce*), è necessario superare il *digital divide*, finanziando e promuovendo progetti tesi alla diffusione delle ICTs anche nelle zone più disagiate. In seguito è stata così istituita la *Digital Opportunity Task Force* (DOT *Force*), che ha presentato un rapporto, dal titolo *Digital Opportunity for All*, in occasione del G8 di Genova del 2001. Interessante è sottolineare la composizione della *DOT Force*: 24 rappresentanti del G8, uno della Commissione europea, 9 dei Paesi in via di sviluppo, 2 per il segretariato (Banca Mondiale e UNDP), 4 di organizzazioni internazionali (Consiglio economico e sociale dell'ONU, ITU, UNESCO, OECD, UNCTAD) e 3 rappresentanti delle *lobbies* imprenditoriali, *World Economic Forum*, GBDE (*Global business and electroniccommercee*) e GIIC (*Global Infor-*

---

in *Diritto dell'Informazione e dell'Informatica*, 2015, 1, pp. 275-314. L'Autore sostiene che «*nel momento in cui l'utente utilizza le tecnologie digitali per esercitare le proprie libertà, diviene contemporaneamente parte (e, talora, anche oggetto) di una transazione economica; e riesce difficile credere che questa dimensione economica, che struttura e condiziona integralmente gli strumenti di esercizio delle libertà, non finisca con l'innervare profondamente le stesse modalità di esercizio della libertà, ciò che da esse ci si attende, i loro effetti, e in ultima analisi il loro stesso contenuto*». Cfr. F. MARCELLI, *Internet fra canale di partecipazione politica e strumento di controllo*, op. cit., p. 14, l'Autore rileva che «*i giganti di Internet* – sono - *beneficate da politiche fiscali e di altro genere che molti governi hanno varato sulla base del presupposto che lo sviluppo della Rete costituisse di per sé un elemento positivo e da favorire*».

[4] V. ZENO-ZENCOVICH, *La intermediazione on-line e la disciplina della concorrenza: i servizi di viaggio, soggiorno e svago*, in *Diritto dell'Informazione e dell'Informatica*, 2015, 2, pp. 43-88. P. MARSOCCI, *Cittadinanza digitale e potenziamento della partecipazione politica attraverso il web: un mito così recente già da sfatare?*, op. cit., p. 51. Cfr. V. ZENO-ZENCOVICH, *La libertà d'espressione. Media, mercato, potere nella società dell'informazione*, Bologna, Il Mulino, 2004, pp. 143-155. SHAPIRO – H.V. VARIAN, *Information Rules*, Cambridge, Massa, Harward Business School Press, 1998. E. NOAM, *Television in Europe*, Oxford, Oxford University Press, 1991, 28 ss.

mation InfrastructureCommission)[5]. Inoltre, quasi in contemporanea a questi eventi, si è svolto sempre nel 2000 a Seattle il *Summit* dei leaders dell'*Internet Economy*, ove è stato rilevato che la povertà è «*una grande opportunità per le aziende operanti nell'ICT*», che mirano in sinergia a ridurre il *digital divide* come un nuovo programma di *business*[6].

Ecco che i processi sociali e politici non sono esenti da questa modificazione sistemica che Internet ha causato, posto che le logiche del mercato digitale hanno pervaso ormai ogni campo di azione. Non sono infrequenti gli utilizzi di metodi e strumenti del ICTs (*Internet Communication Technologies),* come i modelli di *data mining* e *data ware house*, che fanno parte del sistema di *business intelligent*, per raccogliere dati sulle inclinazioni e interessi degli *users*, monitorando i siti di maggiore visualizzazione da parte del singolo utente e realizzando pacchetti di *links* direttamente collegati a questi cui invogliare l'utente a visitare. Saranno gli stessi utenti a ricavare da questi sistemi di profilazione una certa utilità nel proprio vissuto quotidiano.

Internet ha, infatti, cambiato il quotidiano modo di esercitare le proprie libertà e i propri diritti, perché il rapporto tra il singolo e le informazioni e i servizi in esso gravitanti, è divenuto per così dire più individuale, nel senso che apparentemente non vi sono più gli intermediari, che veicolano l'informazione o offrono il servizio, ma il singolo *user* in un rapporto alla pari condivide e raccoglie dati, selezionando autonomamente ciò che è di suo interesse. Si è creata una sorta di consapevole *do ut des* tra gli *users* e i *players* del settore: i primi cedono i propri dati per ottenere un esercizio più rapido delle proprie attività in rete, mentre i secondi offrono in cambio servizi digitali più inclini alle esigenze degli *users*. Per migliorare l'usufruibilità di Internet i *players* hanno affinato le tecniche di manipolazione dei dati inseriti in rete dai singoli *users*, in altre parole creando la c.d. *data governance*.

Per *data Governance* s'intende la definizione delle regole e il controllo sulla gestione dei dati, in termini di pianificazione, esecuzione e monitoraggio. La *data Governance* è dunque la capacità di gestire i dati come un vero e proprio *asset* aziendale, di modo da sfruttare i dati raccolti in rete nel pieno del loro valore economico. Il dato è diventato esso stesso prodotto di mercato, nonché il nuovo "petrolio" dei tempi che stiamo vivendo. Se quanto ivi rilevato appare ormai assodato per l'andamento dei mercati, anche le istituzioni pubbliche, seppur in ritardo iniziano a interessarsi della *data Governance* al fine di creare un *data driver* che sia a vantaggio dello sviluppo dei popoli e non solo dello sfruttamento economico degli stessi, dal momento che in questo modo anche i

[5] Cfr. R. PISA, *Il digital divide e le iniziative per superarlo*, op. cit., 157 ss.

[6] A ciò si aggiunga la realizzazione presso le Nazioni Unite nel 1999, su proposta dell'Italia, del *High Level Panel* di esperti in materie tecnologiche per redigere una relazione, il c.d. *Millenium Report*. Vedi, www.un.org/millennium/assembly.htm. Nel 2005 le Nazioni Unite hanno anche istituito un fondo di solidarietà digitale che prevede la possibilità di dotare l'1% dei contratti del settore pubblico con le società ICTs, ponendo l'obiettivo di connettere il 50% della popolazione mondiale entro il 2015. In parte l'obiettivo è stato raggiunto: due terzi degli utenti di Internet si trovano in aree in via di sviluppo, raddoppiando tra il 2009 e il 2014.

programmi politici e socio-economici possano perseguire nuovi modelli di welfare per essere realizzati sulla base di tali dati condivisi, tra l'altro, dagli stessi utenti.

3. Nuove tecnologie, *data governance* e gli interventi dell'Unione europea

Il concetto di *data Governance* è ormai entrato nel ventaglio concettuale di tutti gli *asset* strategici, anche politici degli Stati e, soprattutto, dell'Unione europea che dal lancio del programma per un *Digital Single Market* ha avviato una serie di iniziative e di programmazioni strategiche che prevedono dieci linee di intervento fondamentale tra cui spiccano, per i nostri fini, l'Economia dei dati e l'*e-government*.

La strategia comunitaria, che guarda al modello statunitense, persegue l'obiettivo di un mercato unico digitale al fine di realizzare un *European Elettronic Communication Code*. I primi passi in questa direzione sono avvenuti con l'approvazione della direttiva 22/2002/CE che tutela gli utenti, come modificata dal successivo *Telecom Package* del 2009[7], e, da ultimo, con il Regolamento UE *Connected Continent*[8], approvato con procedura legislativa ordinaria in codecisione tra Parlamento europeo e Consiglio, rilevando che la scelta dello strumento legislativo del regolamento da parte delle istituzioni europee non deve passare inosservato, perché esso è un atto normativo *self-executing*, per cui ha diretta applicazione negli ordinamenti giuridici degli Stati membri a decorrere dal 30 aprile 2016, data entro la quale gli Stati hanno dovuto inviare alla Commissione europea le proposte di sanzione in caso di violazione della disciplina ivi disposta. In particolare, sono stabili all'art. 1 gli obiettivi del regolamento ovvero quello di «*garantire un trattamento equo e non discriminatorio del traffico nella fornitura dei servizi di accesso a Internet e i relativi diritti degli utenti finali*»[9]. In ciò si apprezza la pregnanza del principio della neutralità della rete per garantire un Internet aperto ovvero si pone il problema principale cioè del *traffic management* o gestione di traffico dei dati fluttuanti in rete. Infatti, vi possono essere sia ragioni tecniche, sia commerciali, e anche politiche, che inducono i fornitori di rete e gli operatori di rete a manipolare il traffico di rete dei dati. Se però la

[7] In materia di tutela degli utenti e protezione dei dati si segnala che il Regolamento 2016/679 abrogherà e sostituirà la direttiva 95/46/CE, a partire dal 25 maggio 2018. V. P. PASSAGLIA, *Privacy e nuove tecnologie, un rapporto difficile. Il caso emblematico dei social media, tra regole generali e ricerca di una specificità*, in *Consultaonline*, 28 settembre 2016; F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali*, vol. II, *Il Regolamento europeo 2016/679*, Torino, Giappichelli, 2016, 9 ss.

[8] Regolamento UE 2015/2120 del Parlamento europeo e del Consiglio, 25 novembre 2015, *che stabilisce misure riguardanti l'accesso a un'internet aperta e che modifica la direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica e il regolamento (UE) n. 531/2012 relativo al roaming sulle reti pubbliche di comunicazioni mobili all'interno dell'Unione*. Si segnala, inoltre, il regolamento n. 531/2012, sulla abrogazione graduale dei sovraprezzi di *roaming* al dettaglio.

[9] Considerando 1 del Regolamento UE 2015/2120.

manipolazione del traffico dei dati in rete può essere giustificata in determinati casi eccezionali come le questioni di sicurezza pubblica o di congestione tecnologica, purché siano casi eccezionali sia per la brevità del caso, sia per ragioni d'interesse preminente secondo il criterio del *best effort*, non si ammettono deviazione nella gestione del traffico per ragioni di carattere commerciale.

Per fronteggiare questi casi di *mala gestio* della rete, il regolamento vi dedica l'intero articolo tre, rubricato "*Salvaguardia dell'accesso a un'Internet aperto*", ove al primo comma si dispone che «*gli utenti hanno il diritto di accedere a informazioni e contenuti e di diffonderli, dal momento che, ai sensi del terzo comma, i fornitori di servizio di accesso a Internet, sono obbligati ad adottare misure di gestione ragionevole del traffico dei contenuti* […]», le quali «*devono essere trasparenti, non discriminatorie e proporzionate*». Il criterio di gestione ragionevole del traffico corrisponde a quello del *best effort* o di ragionevolezza informatica, cioè l'instradamento dei dati risponde alla tipologia di categoria di appartenenza, per cui dati uguali devono essere trattati ugualmente, dati diversi devono essere trattati diversamente. Per esempio, in caso di congestione del traffico è ragionevole privilegiare temporaneamente la trasmissione di una comunicazione istantanea rispetto al caricamento di una pagina web, perché il disagio provocato all'utente è proporzionalmente diverso[10]. Ovviamente, come si dispone nel quarto comma dell'art. 3, si impedisce ai fornitori di bloccare, rallentare, alterare, limitare interferire con l'accesso a Internet degli *users* «*degradando o discriminando tra contenuti specifici*»[11].

Si nota sin da subito che l'Ue persegue il suo obiettivo del mercato unico digitale, c.d. *Digital Single Market*, congegnando un sistema di collaborazione tra pubblico e privato, perché affida ai fornitori dei servizi digitali il compito di garantire l'effettività dei diritti degli *users*, permettendo a questi ultimi comunque di perseguire i propri interessi economici, purché ciò non deprima lo standard di qualità che devono comunque garantire al servizio di accesso basico. Il Regolamento nell'art. 3, par. 5, opera un bilanciamento tra libertà d'impresa e tutela della qualità del servizio per gli utenti prevedendo tre condizioni alle quali gli operatori economici devono sottostare per offrire servizi ottimizzati senza interferire in negativo con il principio della neutralità della rete. La prima condizione è quella di garantire una sufficiente capacità della rete di supportare

[10] Cfr. Considerando 9 del Regolamento UE 2015/2120, per cui «*Il requisito relativo al carattere non discriminatorio delle misure di gestione del traffico non preclude ai fornitori di servizi di accesso a Internet la possibilità di attuare misure di gestione del traffico che distinguono tra categorie di traffico obiettivamente distinte al fine di ottimizzare la qualità complessiva della trasmissione. Al fine di ottimizzare la qualità complessiva e l'esperienza degli utenti, qualsiasi eventuale distinzione di questo tipo dovrebbe essere autorizzata solo sulla base dei requisiti obiettivamente distinti di qualità tecnica del servizio (ad esempio, in termini di latenza, jitter, perdita di pacchetti e larghezza di banda) delle specifiche categorie di traffico e non sulla base di considerazioni di ordine commerciale. Tali misure distintive dovrebbero essere proporzionate rispetto all'obiettivo di ottimizzare la qualità complessiva e dovrebbero trattare allo stesso modo tipologie di traffico equivalenti. Dette misure dovrebbero essere mantenute per il tempo strettamente necessario*».

[11] Art. 4, comma IV, del Regolamento UE 2015/2120 del Parlamento europeo e del Consiglio, 25 novembre 2015. *Ex multis*, E. BIASIN, "Router Freedom" e "Modem *Libero*". *Il diritto di accesso a Internet, la neutralità della rete ed il diritto di scegliere il proprio terminale*, in *Rivista* Medialaws, 6 ottobre 2020.

tanto i servizi d'accesso ad Internet, tanto i servizi aggiuntivi; la seconda condizione impone agli operatori e ai fornitori di rete di non sostituire i servizi d'accesso ad Internet con i servizi aggiuntivi; la terza condizione vieta la riduzione della disponibilità o qualità generale dei servizi d'accesso ad Internet a favore dei servizi aggiuntivi. L'operato dei privati in questo settore è posto così sotto il controllo delle Autorità nazionali, alle quali il regolamento demanda il potere regolamentare di imporre «*requisiti concernenti le caratteristiche tecniche, i requisiti minimi di qualità del servizio e altre misure adeguate e necessarie a uno o più fornitori di comunicazioni elettroniche al pubblico, incluso ai fornitori di servizi di accesso a internet*» (art. 5).

Il percorso già tracciato negli States e dall'Ue è quello di adottare un approccio *case by case* per non imbrigliare a livello normativo l'evoluzione tecnologica del settore del digitale, cercando tuttavia di predisporre strumenti giuridici che siano in grado di tutelare l'esercizio dei diritti e delle libertà fondamentali in rete ed eventualmente sanzionando le violazioni e i comportamenti dannosi da parte degli operatori del settore. Quel che preme sottolineare è che il ruolo delle *Agencies* pare essere cruciale perché esse devono monitorare il comportamento dei fornitori di servizi, affinché questi garantiscano uno *standard* di qualità del servizio di accesso alla rete, il quale fungerà da paramento di giudizio per i casi che si dovessero presentare. Infatti è la diversa qualità del servizio di accesso alla rete che potrebbe interferire con l'esercizio dei diritti degli *users* in rete, nonché aumentare il fenomeno del *digital divide* culturale, perché, se non si garantisse uno standard minimo di accesso che abbia una qualità soddisfacente, il singolo *user* potrebbe essere indotto (e non per libera scelta) a pagare un costo più elevato per ottenere un servizio di accesso quantomeno accettabile[12].

Si ritiene che la regolamentazione dell'Internet che si sta intraprendendo pare essere la soluzione più consona che si ispira alle idee del liberalismo politico e economico, e non agli eccessi del liberismo economico in cui il mercato digitale faceva da padrone. Il liberalismo politico e economico garantisce l'esercizio delle libertà civili, politiche e economiche sotto il controllo vigile delle autorità pubbliche, perché permette, da un lato il rispetto delle caratteristiche principali della rete che si suole sintetizzare nel principio del *innovation without permission*, ovvero ciò che fa del web uno spazio entro il quale le libertà possono esprimere il loro potenziale, di modo da migliorare di volta in volta le innovazioni, dall'altro con il controllo costante da parte di autorità pubbliche in grado di proteggere gli *users* e di perseguire le evoluzioni tecnologiche di pari

[12] In questo senso anche Van Schewick, che sostiene come «*The type of Quality Service interferes with users's ability to use the applications of their choice without interference from network providers and enables network providers to use the provision of Quality of Service as a tool to distort competition among applications within a class, which is exactly what network neutrality rules are designed to prevent*», in B. VAN SCHEWICK, *Network Neutrality and Quality of Serice: What a Nondiscrimination Rule Should Look Like*, op. cit., p. 163.

passo per assicurare un livello di qualità elevata dell'accesso alla rete, che diventa piazza di esercizio delle libertà e dei diritti fondamentali del singolo[13].

Tuttavia, l'Ue per perseguire il DSM Strategy non si è limitata a garantire un accesso più libero alla rete, bensì ha predisposto una serie di interventi legislativi che guidino anche i privati nella raccolta qualitativa dei dati, sempre in un'ottica di condivisione del dato tra pubblico e privato che si è del resto rilevato utile (o avrebbe potuto essere maggiormente utile) per fronteggiare l'emergenza sanitaria[14].

Lungo questo percorso l'intervento più significativo è avvenuto con il regolamento e-iDAS sui servizi di identificazione elettronica, direttive sui contratti pubblici, sui pagamenti, sulle fatture elettroniche), che si pongono l'obiettivo di incoraggiare l'interoperabilità delle soluzioni adottate dalle pubbliche amministrazioni degli Stati membri nella trasformazione digitale, nonché nel rapporto tra le pubbliche amministrazioni e privati.

Tra gli obiettivi della *DSM Strategy* vi è l'aumento di efficienza delle pubbliche amministrazioni e il miglioramento dei servizi pubblici per cittadini e imprese, potenziando i sistemi di identità digitale. Il piano d'azione per l'*e-government* 2016-2020 si concentra infatti su *e-procurement*, registri delle imprese interoperabili, *Single Digital Gateway* per l'accesso ai servizi pubblici; banche dati interoperabili; condivisione dei dati pubblici in ambiente digitale sicuro. *Ergo* anche le istituzioni eurounitarie si accingono a implementare il sistema di gestione dei dati, c.d. *data governance*, per efficentare i servizi al cittadino.

4. *E-government* e i sistemi di identità digitali al servizio dei diritti e libertà fondamentali

Il rapporto tra pubbliche amministrazioni e cittadini è cruciale nei progetti di riforma dell'Ue, tanto da avviare un processo di digitalizzazione della p.a. in tutti gli Stati membri, il cui fine ultimo è quello di garantire un efficientamento dei servizi resi ai cittadini. Per tale ragione è stato ideato il sistema di identità digitale, a partire dalla approvazione del regolamento europeo n. 910 del 23 luglio 2014, c.d. e-iDAS, entrato in vigore il 1 luglio 2016, e, in Italia, con la realizzazione dello SPID, previsto nel d.lgs. n. 82, del 7 marzo 2005 e successive modifiche (da ultimo il d.lgs. 26 agosto 2016, n.179), e a cui è stato dato attuazione con il d.p.c.m. 24 ottobre 2014.

Il sistema di identificazione elettronica è stato oggetto di normazione con la direttiva del 1999/93/CE e, poi abrogata dal regolamento e-iDAS. Il re-

[13] Cfr. *BEREC Guidelines on the Implementation by National Regulators of European Net Neutrality Rules*, agosto 2016.

[14] Al momento in cui si scrive è in corso il dibattito pubblico sulla funzionalità e utilità delle app pubbliche per il *contact tracing* e inoltre si rimarca la necessità di instaurare una *partenership* con Google per la condivisione dei dati sanitari e gli spostamenti delle persone fisiche. Cfr., A. LONGO, *L'*App *Immuni cambia. Seguirà il modello decentralizzato di* Apple *e* Google, in www.ilsole24ore.it, 22 aprile 2020; F. APERIO BELLA, *L'accesso alle tecnologie innovative nel settore salute tra universalità e limiti organizzativi (con una postilla sull'emergenza sanitaria)*, in *Rivista PA, Persona e Amministrazione*, 2020, 1, pp. 219-245.

golamento e-iDAS ha come obiettivo quello di eliminare le barriere transfrontaliere dei mezzi di identificazione elettronica utilizzata negli Stati almeno per l'autenticazione dei servizi pubblici resi al cittadino. É emerso che per raggiungere tale obiettivo, la nuova disciplina è incentrata sulla necessità di garantire effettivamente la sicurezza della trasmissione e condivisione dei dati, nonché una maggiore fruibilità per i soggetti di diritto, tanto persone fisiche, tanto persone giuridiche, dei servizi pubblici *on line* che ogni Stato offre all'interno del proprio spazio nazionale, ma che aspira ad offrire in un'ottica transfrontaliera per raggiungere un mercato unico digitale[15]. All'art. 8, par. 7, si delega alla Commissione europea il compito di emanare linee guida che determino i tre livelli di sicurezza che devono essere garantiti nell'interoperabilità dei servizi di identificazione elettronica tra Stati membri, quali il livello basso, significativo ed elevato, prevedendo una gradazione crescente dei controlli tecnici per ridurre il rischio di uso abusivo o alterazione dell'identità. In particolare, la Commissione ha emanato la decisione n. 296 del 24 febbraio 2015 al fine di garantire procedure semplificate di "revisione *inter pares*" tra gli Stati membri che intendono accedere a questo sistema di cooperazione ed interoperabilità unionale dei regimi di sicurezza di identificazione elettronica[16], posto che il riconoscimento reciproco degli strumenti di identificazione *on-line* è obbligatorio per il settore pubblico, mentre è concepito come una facoltà per il settore privato, e, successivamente, la decisione n. 1502 dell'8 settembre 2015, con la quale la Commissione ha stabilito le specifiche tecniche dei livelli di sicurezza garantiti ponendo come *vademecum* iniziale il ISO/IEC 29115, quale principale norma internazionale disponibile in materia di livelli di garanzia per i mezzi di identificazione elettronica[17].

Un ulteriore passo in avanti è stato quello di infondere fiducia nei sistemi di identità digitale e nel loro utilizzo da parte dei cittadini. Al riguardo, la Commissione ha approvato il Regolamento di esecuzione 2015/806 del 22 maggio 2015, col quale ha definito le specifiche relative alla forma del marchio di fiducia UE per i servizi fiduciari qualificati. In particolare, il regolamento n. 910/2014, dispone che i prestatori di servizi fiduciari qualificati possano utilizzare un marchio di fiducia per i servizi fiduciari qualificati per incrementare la fiducia in tali servizi e la facilità d'uso per gli utenti. Lo scopo del marchio di fiducia è proprio quello di rendere immediatamente intellegibili e identificabili

[15] Cfr. G. FINOCCHIARO, *Una prima lettura del reg. UE n. 910/2014 (c.d. eIDAS): identificazione on line, firme elettroniche e servizi fiduciari*, in *Nuove Leggi Civ. Comm.*, 2015, 3, 419 ss.

[16] DECISIONE DI ESECUZIONE (UE) 2015/296 DELLA COMMISSIONE *del 24 febbraio 2015 che stabilisce modalità procedurali per la cooperazione tra Stati membri in materia di identificazione elettronica a norma dell'articolo 12, paragrafo 7, del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno.*

[17] Considerando 3, REGOLAMENTO DI ESECUZIONE (UE) 2015/1502 DELLA COMMISSIONE *dell'8 settembre 2015 relativo alla definizione delle specifiche e procedure tecniche minime riguardanti i livelli di garanzia per i mezzi di identificazione elettronica ai sensi dell'articolo 8, paragrafo 3, del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno.*

da parte degli utenti i servizi fiduciari qualificati rispetto ad altri servizi fiduciari, contribuendo in tal modo alla trasparenza nel mercato e, conseguentemente, favorendo la fiducia nei servizi on-line e la loro facilità d'uso. È uno *step* definito dalla stessa Commissione fondamentale, «*affinché gli utenti possano beneficiare appieno dei servizi elettronici e se ne avvalgano consapevolmente*»[18], come del resto si ribadisce nell'art. 4 del medesimo Regolamento di esecuzione.

A questi interventi si aggiungono inoltre a completamento del sistema e-iDAS, la decisione esecuzione (UE) 2015/1506 della Commissione dell'8 settembre 2015 che stabilisce le specifiche relative ai formati delle firme elettroniche avanzate e dei sigilli avanzati che gli organismi del settore pubblico devono riconoscere, di cui all'articolo 27, paragrafo 5, e all'articolo 37, paragrafo 5, del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno; nonché la decisione di esecuzione (UE) 2016/650 della Commissione del 25 aprile 2016 che definisce le norme per la valutazione di sicurezza dei dispositivi per la creazione di una firma e di un sigillo qualificati a norma dell'articolo 30, paragrafo 3, e dell'articolo 39, paragrafo 2, del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno.

Il sistema unionale di identificazione elettronica, così come congeniato dalle istituzioni eurounitarie, si erge dunque su due pilastri fondamentali, la garanzia della sicurezza del sistema e l'efficentamento dei servizi pubblici on-line, nel pieno rispetto prima della direttiva 95/46/CE sul trattamento dei dati personali, e successivamente del Regolamento Privacy, che ha abrogato e sostituito la direttiva privacy[19]. Per raggiungere questo obiettivo si è strutturato un sistema *in progress* che sarà oggetto di verifiche da parte delle autorità di vigilanza nazionali ed europee, al fine di presentare al Parlamento europeo e al Consiglio i risultati raggiunti entro il 2020. Il metodo del controllo periodico si rivela molto utile per testare l'impatto dei sistemi di identificazione elettronica sulla tutela della identità personale e l'efficentamento dei servizi pubblici in rete, anche in relazione alla nuova disciplina eurounitaria sul trattamento dei dati personali, soprattutto con riferimento alle definizioni nella materia in oggetto all'art. 3 del regolamento e-iDAS. Quel che preme ivi rilevare è che per la Commissione la cartina di tornasole per verificare il buon esito di funzionamento del sistema di identità digitale su scala eurounitaria è quella di aver innescato la "fiducia" in tale sistema da parte dei cittadini per invogliarli ad utilizzare i servizi pubblici on-line. È un nodo cruciale quello fiduciario che si annida

[18] Regolamento di esecuzione (UE) 2015/806 del 22 maggio 2015, che stabilisce le specifiche relative alla forma del marchio di fiducia UE per i servizi fiduciari qualificati.

[19] Il nuovo regolamento UE 2016 (679) del Parlamento e del Consiglio del 27 aprile 2016, *relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)*», entrato in vigore nel maggio 2016, ma applicabile a partire dal maggio 2018 secondo il disposto dell'art. 99, comma 2.

nel rapporto tra pubbliche amministrazioni e cittadini e che trasla dunque anche nel digitale. Se i cittadini hanno fiducia in tali sistemi di identità digitali, saranno predisposti ad utilizzare i servizi pubblici on-line. Questo non è uno scoglio di poco conto da superare, soprattutto se si tiene conto che a livello empirico gli utenti del web si fidano maggiormente dei *players* privati, piuttosto che delle istituzioni per esercitare i propri diritti e libertà in rete. L'unico modo per innescare fiducia nei cittadini sul buon uso dei sistemi di identità digitale è quello di incrementare le risorse per garantire elevati sistemi di sicurezza e, soprattutto, garantire il funzionamento efficiente dei servizi pubblici on-line.

4.1. Il sistema di identità digitale italiano e la tutela dei dati

La Repubblica italiana si è da sempre posta tra i primi Stati a livello europeo nel prevedere a livello legislativo il sistema di identità digitale c.d. SPID. Lo SPID è stato introdotto nell'ordinamento italiano già nel 2005 con l'art. 64 del CAD, da modificato dal d.lgs. n. 179 del 2016. In particolare, dall'articolo 64, comma 2-*ter*, si ricava una definizione *in nuce* di cosa si debba intendere per SPID: esso «*è costituito come insieme aperto di soggetti pubblici e privati che, previo accreditamento da parte dell'AgID, secondo modalità definite con il decreto di cui al comma 2* sexies*, identificano gli utenti per consentire loro l'accesso ai servizi in rete*»[20]. Pertanto, il sistema SPID ha una doppia natura funzionale: è sia un sistema di identificazione, sia un sistema di accesso ai servizi in rete.

È innanzitutto un sistema di identificazione a cui si suole aggiungere l'aggettivo "digitale", cogliendo l'evoluzione dei tempi che registrano la creazione di una vita "digitale" dei soggetti giuridici accanto alla vita "reale". Al riguardo, il d.lgs. n. 179 del 2016 elabora, in parte, quanto già espresso nell'art. 1, lett o) del d.p.c.m del 24 ottobre 2014: una definizione di identità digitale. In particolare, dispone all'art. 1, lett. u-*quater*, che l'identità digitale è «*la rappresentazione informatica della corrispondenza tra un utente e i suoi attributi identificativi, verificata attraverso l'insieme dei dati raccolti e registrati in forma digitale secondo le modalità fissate nel decreto attuativo dell'articolo 64*»[21].

Il sistema SPID, in vigore già dall'aprile 2016, è dunque un sistema federato di gestione dell'identità digitale che consente ai soggetti giuridici, persone fisiche e giuridiche, di utilizzare le medesime credenziali per l'accesso ai servizi in rete forniti da diversi fornitori sia privati, che pubblici, perseguendo gli obiettivi che già erano stati posti nel CAD. Si prevede, inoltre, l'obbligo per tutti i soggetti qualificati dall'art. 3 del decreto ministeriale come "partecipanti

[20] V. AMENTA, A. LAZZARONI, L. ABBA, *L'identità digitale: dalle nuove frontiere del Sistema Pubblico di Identificazione (SPID) alle problematiche legate al web*, in *Ciberspazio e diritto*, vol. 16, n. 52, 1, 2015, pp. 11-28. G. FINOCCHIARO, *La protezione dei dati personali e la tutela dell'identità*, in AA.VV., *Diritto di Internet*, UTET GIURIDICA, 2014, pp. 151-181. A. PRINCIPATO, *Verso nuovi approcci alla tutela della privacy: privacy by design e privacy by default settings*, in *Contratto e impresa*, 2015, 1, pp. 197-227.

[21] La regolamentazione dello SPID è reperibile nel d.p.c.m. del 24 ottobre 2014, dal quale si ricavano le norme che stabiliscono i livelli di autenticazione informatica progressivamente crescenti in termini di sicurezza, stabiliti all'art. 6 del decreto ministeriale.

allo SPID" di aderirvi, posto che le pubbliche amministrazioni sono state obbligate a prendere parte al sistema SPID entro 24 mesi dall'accreditamento del primo gestore dell'identità digitale, avvenuto con delibera di *Accredita* del 28 giugno 2016.

Del resto, il nuovo CAD qualifica come un diritto, per l'appunto, l'assegnazione di un'identità digitale ai sensi dell'art. 3, 1 *quinques*, per *tutti i cittadini e le imprese*, nonché, ai sensi del comma 1 *sexies*, per *tutti gli iscritti all'Anagrafe nazionale della popolazione residente*[22]. Quanto ivi rivelato, dimostra che il sistema di SPID è funzionale ai diritti e alle libertà fondamentali dei cittadini, perché concretizza il diritto degli stessi di esercitare tali prerogative anche nel web. Lo SPID pare rafforzare in rete l'esercizio effettivo dei diritti del singolo soggetto giuridico, il quale è messo realmente nelle condizioni di poter gestire autonomamente la propria identità digitale, ed accedere ai servizi pubblici on-line, al pari di quando usufruisce delle piattaforme digitali private per esigenze non istituzionali.

La differenza da rimarcare tra l'utilizzo dello SPID per usufruire dei servizi pubblici (*rectius* per esercitare i propri diritti) e l'utilizzo delle piattaforme digitali dei *players* privati, risiede non a caso nella maggior tutela di sicurezza dei dati immessi dal singolo, nonché nella usabilità degli stessi.

La raccolta e la condivisione dei dati personali tramite SPID tra i gestori delle identità digitali, i fornitori dei servizi in rete e gli *users*, non sono oggetto di profilazione. Questo sta ad indicare che tali dati sono tutelati pienamente e che non potranno essere oggetto di cessione o scambio economico per fini diversi da quelli istituzionali per i quali ogni singola istituzione pubblica ha richiesto il rilascio per l'accesso al servizio pubblico offerto in rete. Ciò si evince dal combinato disposto degli artt. del CAD e della normativa *privacy* cui espressamente rinvia l'art. 2, comma V, del CAD. In particolare l'art. 44 del CAD, disponendo i requisiti per la gestione e conservazione dei documenti informatici alla lettera f) del comma I, prevede l'obbligo per i gestori di garantire l'accesso in condizioni di sicurezza alle informazioni del sistema nel rispetto delle disposizioni in materia di tutela dei dati personali, tra i quali rientrano i dati sensibili e i dati giudiziari la cui trasmissibilità tra pubbliche amministrazioni può avvenire solo se previsto da legge, nelle modalità ivi previste e solo per fini istituzionali. Da ciò si esclude che i dati sensibili dei soggetti che accedono a SPID siano oggetto di profilazione, dato l'espresso divieto del Codice *privacy*, come modificato dal Regolamento 2016/679, cui si rinvia interamente per la disciplina del trattamento dei dati personali[23]. Ergo l'integrità della identità del singolo e i dati sensibili continuano ad avere una tutela giuridica e informatica maggiore rispetto agli altri dati che sono già più facilmente accessibili dai terzi.

Al riguardo, si noti che nei successivi artt. 50 e 51, comma II, del CAD, si dispone che i documenti informatici delle pubbliche amministrazioni devono essere custoditi e conservati per garantire l'integrità, la riservatezza, ed evitare

[22] D.lgs. n. 179 del 2016, art. 3, comma 1 *quinques*.

[23] E.C. PALLONE, *La profilazione degli individui connessi a Internet:* privacy online *e valore economico dei dati personali*, in *Ciberspazio e diritto*, vol. 16, n. 53, n. 2, 2015, pp. 295-327.

l'utilizzo abusivo degli stessi, fuori dai limiti consentiti per le finalità espresse da legge, ovvero le p.a. potranno condividere i dati, grazie al sistema SPID (che è un sistema federato di accesso ai servizi erogati in rete dalle pubbliche amministrazioni e tra pubbliche amministrazioni), esclusivamente per i loro fini istituzionali tramite l'ausilio del sistema pubblico di connettività (SPC).

Si ricordi che è stato di recente approvato il nuovo regolamento UE 2016 (679) del Parlamento e del Consiglio del 27 aprile 2016, entrato in vigore nel maggio, ma applicabile a partire dal maggio 2018 secondo il disposto dell'art. 99, comma 2. Il presente regolamento, «*relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)*», ha modificato la precedente normativa in materia di trattamento di dati personali con una ricaduta notevole sulle legislazioni nazionali al fine di uniformare la normativa in questione su scala eurounitaria[24]. Si pone all'evidenza sin da subito che il detto regolamento presenta come criteri-guida la minimizzazione dell'uso dei dati e la limitazione delle finalità di utilizzo nei sistemi di identificazione e autenticazione digitali, come espressamente sancito nell'art. 5, lett. b) e c)[25].

5. *Digital transformation*, *e-government* e *data governance* al servizio dei diritti e delle libertà fondamentali

L'obiettivo che si persegue è dunque quello di rendere concretamente fruibile l'amministrazione digitale, di cui lo SPID ne è un'asse portante[26]. Del resto, Ai sensi dell'art. 2, comma 2, del CAD, tutte le pubbliche amministrazioni sono state tenute ad adeguarsi al sistema SPID entro 24 mesi dal primo accreditamento.[27]

In particolare si parla di *digital first*, ovvero l'obbligo per le p.a. di sostituire gli attuali procedimenti in formato cartaceo con quelli in formato digitale[28]. I regolamenti attuativi offrono un panorama normativo in questo senso incrementando i diritti digitali di cittadini ed imprese, già previsti nell'artt. 3 e 12 del CAD e nel nuovo art. 3 bis della l. n. 241 del 1990, ove si dispone che «*per conseguire maggiore efficienza nella loro attività, le amministrazioni pubbliche incentivano l'uso della telematica, nei rapporti interni, tra le diverse amministrazioni e tra queste e i privati*»[29].

[24] P. PASSAGLIA, Privacy *e nuove tecnologie, un rapporto difficile. Il caso emblematico* dei social media*, tra regole generali e ricerca di una specificità*, in *www.giurcost.it*, 28 settembre 2016, fasc. n. 3.

[25] Regolamento UE 2016 (679) del Parlamento e del Consiglio del 27 aprile 2016: Articolo 5 - Principi applicabili al trattamento di dati personali.

[26] F. BRUGALETTA, *Lo stato di informatizzazione della p.a. in Italia e in Europa*, in *Diritto dell'Internet*, op. cit., pp. 691-712. F. Cardarelli, *Amministrazione digitale, trasparenza e principio di legalità*, in *Diritto dell'informazione e dell'informatica*, 2015, 1, pp. 227-273.

[27] V. www.agid.com. *Ex multis*, P. FORTE, *Diritto amministrativo e data science. Appunti di intelligenza amministrativa digitale*, in *Rivista Pa, Persona e Amministrazione*, 2020, 1, pp. 247-300.

[28] Cfr. d.p.c.m. 13 novembre 2014, pubblicato in Gazzetta Ufficiale n. 8 del 12 gennaio 2015.

[29] V. anche l'art. 12 del CAD.

In ciò si inserisce il fenomeno della *digital transformation* che sta interessando anche la pubblica amministrazione. L'Italia con la dichiarazione ministeriale sull'*e-Government* sottoscritta a Tallin nell'ottobre 2017, ha impegnato il nostro Paese, così come gli altri Stati Membri, alla realizzazione dei principi e degli obiettivi dell'*e-Government Action Plan 2016-2020*, che è parte integrante della strategia del *Digital Single Market* europeo. Al riguardo si parla di *e-government* ovvero di amministrazione digitale che persegue tutte le attività di diffusione di informazioni ed erogazione di servizi che il sistema pubblico realizza grazie all'ausilio delle reti telematiche (in particolare della rete Internet), sfruttando il sistema di identità digitale. L'*e-government* abbraccia sia i rapporti tra le amministrazioni pubbliche e cittadini e le imprese, sia i rapporti tra le amministrazioni pubbliche stesse, garantendo un sistema di interoperabilità e di comunicazione efficiente dei dati tra pubbliche amministrazioni. In questo modo i dati circolano all'interno del sistema pubblico informatico, garantendo un efficentamento dei servizi pubblici a favore del cittadino. Si pensi a titolo di esempio come migliora il servizio di rilascio di documenti, se le amministrazioni pubbliche condividono e validano vicendevolmente a livello informatico i dati presenti nei rispettivi *database*[30].

Tuttavia, il timore che le banche dati in possesso delle p.a. e dei gestori delle identità digitali possono essere piegati ad interessi ultronei, genera scetticismo per la tutela delle identità dei singoli. Se tale timore trova riscontro nei vari episodi di hackeraggio[31], non deve distogliere l'attenzione dal miglioramento in termini di qualità della vita e di esercizio dei diritti che le nuove tecnologie offrono, ma deve concentrarsi sulla creazione di un sistema di responsabilità in caso di disservizio seguendo lo sviluppo delle tecnologie della sicurezza informatica. Dello stesso avviso pare essere la giurisprudenza amministrativa che sanziona le amministrazioni inadempienti rispetto all'adeguamento all'Agenda digitale, e individua come responsabili in caso di mal funzionamento delle piattaforme digitali i soggetti pubblici che erogano servizi *on line*[32]. A tal fine la Corte dei conti ha ritenuto responsabili per danno erariale i dirigenti pubblici di un ente locale, che non abbiano raggiunto negli indici di risultato per l'assolvimento degli obblighi di incremento di pubblicità e trasparenza, pur percependo l'indennità di risultato[33], mentre il Tar Puglia è andato oltre, stabi-

[30] A. SACCHI, F SQUARTINI, *L'(in)efficienza del settore pubblico e il ruolo dell'*e-government, in *Rivista di economia, cultura e ricerca sociale*, 2019, 14, pp. 25-53.

[31]Si pensi al caso del sito INPS in piena emergenza sanitaria dello scorso marzo 2020, quando i dati di milioni di cittadini vennero resi pubblici per errore per aver fatto richiesta online di riconoscimento del bonus di 600 euro. *Ex multis*, A. ROCIOLA, P. FIORE, *Sito dell'Inps in tilt. "Attacco hacker". Ma analisti lo escludono*, in *www.agi.it*, 01 aprile 2020.

[32] Cfr. T.A.R. Trentino, 15 aprile 2015, n. 149. In particolare il giudice amministrativo ha ritenuto responsabile tanto l'ideatore della piattaforma che non abbia procedura a risolvere le eventuali anomalie di funzionamento, tanto il pubblico funzionario che, informato delle anomalie, non abbia proceduto tempestivamente le attività necessarie per accogliere le istanze del richiedente. Vedi anche, T.A.R. Friuli Venezia Giulia, Sez. I, 24 novembre 2015, n. 523; T.A.R. Puglia- Bari, Sez. I, 18 dicembre 2015, n. 1646.

[33] Corte dei conti Lazio, 2 febbraio 2015.

lendo che è onere della pubblica amministrazione assumersi il rischio dei malfunzionamenti e degli esiti anomali dei sistemi informatici di cui la stessa si avvale[34].

La giurisprudenza amministrativa affronta i problemi che un sistema di gestione di identità digitale può causare, facendo trasparire una consapevolezza nei giudici ovvero che l'amministrazione digitale deve essere pienamente perseguita e che non sono più accettati i comportamenti remissivi delle p.a. che si trincerano dietro le problematiche della tutela della sicurezza dei dati in rete. In particolare, quanto ivi sostenuto sembra ampiamente trasparire dal Rapporto sull'informatica pubblicato della Corte dei Conti[35], che richiama le determinazioni dello OECD nel *Multilingual Summaries OECD Digital Economy*. L'OECD ha sottolineato infatti che «*L'innovazione digitale e i nuovi modelli imprenditoriali stanno trainando la trasformazione, specie dei posti di lavoro e degli scambi commerciali. L'innovazione basata sui dati, i nuovi modelli imprenditoriali e le applicazioni digitali stanno modificando il funzionamento della scienza, dei governi, delle città, e di settori come la sanità e l'agricoltura*»[36].

È evidente che le Amministrazioni devono offrire servizi on-line semplificati, in grado di consentire ad un'ampia platea di utenti un esteso e più facile utilizzo dei servizi stessi. L'e-*government* e la *data governance* pubblica svolgono un ruolo trainante per lo sviluppo del Paese sia dal punto di vista economico che culturale, portando l'attività amministrativa a massimizzare il rispetto dei canoni di efficienza ed economicità.

Al riguardo illuminante è la pronuncia del Consiglio di Stato n. 2270 del 9 aprile 2019, che sostiene «in generale non può essere messo in discussione che un più elevato livello di digitalizzazione dell'Amministrazione pubblica sia fondamentale per migliorare la qualità dei servizi resi ai cittadini e agli utenti (…). L'utilizzo di procedure di digitalizzazione nella gestione dell'interesse pubblico sia conforme ai canoni di efficienza ed economicità dell'azione amministrativa (art. 10, comma 1, della l. n. 241/1990), i quali, secondo il principio costituzionale del buon andamento dell'azione amministrativa (art. 97 Cost.), impongono all'amministrazione il conseguimento dei propri fini con il minor dispendio di mezzi e risorse e attraverso lo snellimento e l'accelerazione dell'iter procedimentale».

Secondo la Corte dei conti è necessario un approccio organico che sviluppi una *data governance* pubblica per favorire la possibilità dei cittadini, delle istituzioni e delle imprese, di fornire i dati una sola volta all'amministrazione «che abbia esigenza di disporne (c.d. principio del *once only*), con ciò consenten-

[34] Cfr. T.A.R. Puglia, 28 luglio 2015, n. 1094. V., G. SGUEO, *L'Amministrazione digitale*, in *Giornale di Diritto Amministrativo*, 2016, 1, 114 ss. B. BARMANN, *La responsabilità della amministrazione per il cattivo funzionamento dei sistemi informatici – il commento*, in *Giornale di Diritto Amministrativo*, 2016, 3, 393 ss.

[35] Corte dei conti, sezioni riunite in sede di controllo, *Rapporto sull'informazione pubblica*, settembre-ottobre 2019.

[36] *https://www.oecd-ilibrary.org/science-and-technology/oecd-digital-economy-outlook-2017/summary/italian_6553fcf7-it;jsessionid=t4n40Tmb8SnY_BuXhC5YX XTC.ip-10-240-5-111.*

do la fattiva realizzazione dell'interoperabilità e della gestione del "dato", certo e condiviso, con i conseguenti benefici in termini di efficienza della Pubblica amministrazione»[37]. Le nuove tecnologie sono dunque diventate strumenti di inclusione nel rapporto tra cittadini e p.a., facilitando l'esercizio dei diritti dei singoli e migliorando l'efficacia dell'apparato amministrativa. Strumentali a tale obiettivo sono i sistemi di identità digitale, come SPID, perché ciascun individuo con le stesse credenziali d'accesso potrà autonomamente gestire i propri rapporti con le p.a.; inoltre, le p.a. aumenteranno i propri canali di interoperabilità e comunicazione dei dati, efficentando i servizi pubblici e riducendo i costi di gestione.

6. La *digital transformation* e l'esercizio di diritti fondamentali e delle libertà personali: compressione o miglioramento? Criticità e prospettive ai tempi del Covid-19

Il fenomeno epocale della pandemia generata dalla diffusione del virus Covid-19 sta velocemente rimescolando le carte delle certezze (o presunte tali) su cui gli Stati si ergevano e reggevano. Un evento così prolungato ha avuto almeno il merito di aver posto l'attenzione degli Stati sulle tematiche legate alle nuove tecnologie, non più soltanto da un punto di vista economico, ma soprattutto dal punto di vista della concretezza dell'esercizio dei diritti e delle libertà fondamentali.

Seppur gli Stati e le istituzioni sovranazionali avessero da tempo intrapreso strategie "*digital*", anche per contrastare il potere geopolitico che i *players* del settore sono già in grado di esercitare, il dato lampante è che siamo ancora molto indietro sul fronte della garanzia dell'esercizio dei diritti e delle libertà fondamentali in rete. Infatti il massiccio utilizzo delle nuove tecnologie e soprattutto, dell'accesso ad Internet, nel periodo della pandemia, ha acuito, questa volta in positivo, un dato rilevante: le nuove tecnologie incrementano le possibilità di accesso al patrimonio conoscitivo e ai servizi, non solo in termini quantitativi perché il numero dei soggetti che accedono ad Internet è su scala globale, ma soprattutto in termini di facilitazione all'usufruibilità dei servizi online, offerti sia dai poteri pubblici che dai privati.

Quanto rilevato evidenzia l'importanza strategica dell'accesso ad Internet per accedere al patrimonio digitalizzato della conoscenza e dei servizi direttamente connessi ai diritti e le libertà fondamentali, tale da riaccendere i riflettori su una questione dibattuta ormai da quasi un decennio: l'accesso ad Internet è un diritto fondamentale perché permette e agevola l'esercizio dei diritti e delle libertà della persona, permettendo al singolo di goderne e di stimolare la propria personalità[38].

[37] Corte dei conti, sezioni riunite in sede di controllo, *Rapporto sull'informazione pubblica*, settembre-ottobre 2019, 5 ss.

[38] O. POLLICINO, G. ROMEO (a cura di), *The Internet and Constitutional Law: The protectiom of fundamental rights and constitutional adjudication in Europe*, London and New York, 2016. T. E. FROSINI, *Libertè, Egalitè, Internet*, editoriale, in *Percorsi costituzionali*, 2014, 2, p. 3. Corte Supre-

Tuttavia, se da una parte l'emergenza Covid-19 ha avuto il merito di accelerare il processo di digitalizzazione dei servizi pubblici e della pa, attraverso l'utilizzo massimo della *data governance* e l'implementazione dei sistemi di identità digitale, dall'altra ha tagliato fuori da questa rivoluzione intestina tutta quella fetta della popolazione che non può accedere ad Internet per problemi economici e mancanza delle dotazioni strumentali adeguate, pensiamo agli studenti di ogni ordine e grado e alle problematiche connesse alla DAD ovvero didattica a distanza, o a chi non ha i mezzi economici per accedere ai servizi pubblici online tramite i sistemi di identità digitale (si pensi alla necessità di SPID per accedere al bonus 600 euro), oppure per chi non è in grado di accedere ad Internet perché non ha sviluppato le capacità e le conoscenze digitali, tra tutti si pensi alla popolazione più anziana. Il *digital divide* è un problema che gli Stati europei stanno cercando di arginare, come si evince dal *Digital Economy and Society Index* (DESI), della Commissione europea, ma l'Italia non appare certamente tra i Paesi più virtuosi.

Il DESI 2019 evidenzia la situazione dell'evoluzione digitale in Europa, dimostrando che le politiche avviate dalla Commissione per un unico grande mercato digitale non sono ancora in grado di soddisfare le aspettative. In particolare, l'indice DESI rileva i progressi compiuti dagli Stati membri in termini di digitalizzazione su cinque dimensioni, quali: a) connettività; b) capitale umano; c) uso dei servizi internet da parte dei cittadini; d) integrazione delle tecnologie digitali; e) servizi pubblici digitali. Ogni dimensione è l'insieme di indicatori che, analizzati singolarmente, permettono di comprendere l'evoluzione nel tempo della competitività digitale di ciascuno Stato membro, in comparazione con gli altri Stati[39].

---

ma federale degli Stati Uniti d'America, *Reno* v. *American Civil Liberties Union*, 521 U.S. 844. Cfr. V- ZENO ZENCOVICH, traduzione, in *Rivista dell'Informazione e dell'Informatica*, 1996, 604 ss. P. COSTANZO, *Profili costituzionali di internet*, in E. TOSI (a cura di), *Diritto di internet e dell'e-business*, III ed., Milano, Giuffrè, tomo I, 74 ss. *Conseil constitutionnel*, *décision* n. 2009-580 DC, 10 giugno 2009, *considérant* 12. La sentenza è consultabile in lingua italiana in *Diritto dell'Informazione e dell'Informatica*, 2009, 525 ss. Vedi, P. PASSAGLIA, *L'accesso ad Internet è un diritto (il* Conseil constitutionnel *francese dichiara l'incostituzionalità di parte della c.d.* "legge anti file-sharing*)*, in *Foro.it*, IV, 473. Molte Costituzioni di terza generazione costituzionalizzano il diritto di accesso ad Internet, in particolare, si annoverano la Costituzione greca del 2001, che all'art. 5, statuisce che «*All persons are entitled to participate in the Information Society. Facilitation of access to electronically handled information, as well as of the production, exchange and diffusion there of constitutes an obligation of the State, always in observance of the guarantees of articles 9, 9A and 19*»; la Costituzione dell'Honduras, il cui art. 182 parla espressamente di *habeas data*; la Costituzione del Venezuela che all'art. 108 obbliga lo Stato a garantire «*servicios públicos de radio, televisión y redes de bibliotecas y de informática, con el fin de permitir el acceso universal a la información*». E infine, l'art. 16, comma 3, della Costituzione dell'Ecuador che riconosce espressamente «*El acceso universal a las tecnologías de información y comunicación*». Vedi, G. D'IPPOLITO, *La proposta di un art. 34-bis in Costituzione*, in M.R. ALLEGRI, G. D'IPPOLITO, (a cura di), *Accesso a Internet e neutralità della rete fra principi costituzionali e regole europee*, 2017.

[39] Il DESI è consultabile al seguente sito: https://ec.europa.eu/digital-single-market/en/shaping-digital-single-market.

L'Italia si colloca al 25° posto del 2018 al 24 del 2019, su 28 Paesi, permanendo sotto la media EU, a causa di problemi strutturali che incidono sul risultato complessivo, nonostante si rilevi una tendenziale crescita in alcune aree indicizzate dal DESI. Migliora invece sul fronte della "Connettività" (da 26esimi dello scorso anno a 19esimi) e dei "Servizi pubblici digitali" (da 19esimi a 18esimi).

Il dato più preoccupante è quello relativo alla dimensione "*uso dei servizi internet da parte dei cittadini*", perché l'Italia si colloca al 25° posto senza che si siano registrati margini di miglioramento. In specie, mentre sono stati registrati lievi aumenti nello *shopping online* (dal 44 per cento degli utilizzatori di internet al 47 per cento, contro una media europea del 69 per cento), non vi è un miglioramento sull'utilizzo dei servizi pubblici on-line. In particolare la categoria degli "utenti *e-Government*" è la peggiore, perché l'Italia si classifica al penultimo posto in classifica fra i paesi UE. La ragione non è attribuibile soltanto alla bassa "alfabetizzazione digitale", bensì anche alla scarsa qualità dei servizi offerti on-line dalle pa perché poco accessibili e poco *user-friendly*. Come evidenziato dalla Corte dei conti «*l'utilità, l'usabilità e la facilità di utilizzo rappresentano una forte motivazione per avvicinare i cittadini ad adottare i servizi digitali*».

Traendo le fila e cercando di dare una risposta alla domanda posta *in limine* pare evidente che le nuove tecnologie sono sia un miglioramento, che una compressione dei diritti delle libertà fondamentali. Il miglioramento nell'esercizio degli stessi per il tramite delle nuove tecnologie è evidente, ma solo se gli Stati si dotano di strutture adeguatamente organizzare sia a livello infrastrutturale, sia a livello di conoscenze e di capitale umano da impiegare nel settore. Ma ciò comunque non basterebbe. La *digital transformation* anziché diventare veicolo di miglioramento dell'esercizio dei diritti, rischia di diventare un blocco agli stessi, appunto una intollerabile compressione dell'esercizio dei diritti fondamentali, come del testo l'attuale emergenza sanitaria ha portato a galla: famiglie prive di dotazione strumentali per affrontare le sfide del *lockdown*.

Gli Stati devono carpire il dato storico ovvero che il sistema di *Welfare* e, dunque, di garanzia dell'effettività dei diritti, ha futuro solo se si intraprende seriamente la via del digitale. L'effettività dei diritti e delle libertà fondamentali passa oramai per la via del digitale, che deve essere strutturata per non perdere le garanzie acquisite in termini di tutela del singolo individuo. Non cogliere tali sollecitazioni, significherebbe rinunciare allo sviluppo socioculturale ed economico dei popoli.