RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318
Fascicolo 1-2022
DOI: 10.32091/RIID0068
Articolo sottoposto a peer review

Internet governance: una questione di digital trust

Igor Marcolongo • Lorenzo Piatti • Alessandra Bossi

Ci sono due pilastri fondamentali che oggi garantiscono una rete Internet forte basata su una governance affidabile e utilizzabile a livello globale: regolamentazione e identità digitale. L'evoluzione di Internet sarà descritta partendo da questi due strumenti abilitanti del trust digitale. Sotto il primo aspetto, inizialmente si analizzerà il significato e l'impatto che la Internet governance ha avuto a livello teorico-filosofico, investigando il rapporto tra legge e codice, e in seguito sarà esaminato in concreto ciò che è stato portato avanti dai legislatori italiano ed europeo, che hanno da tempo cercato la migliore formula normativa per garantire un ecosistema in grado di bilanciare gli interessi dei cittadini e del mercato. Il secondo aspetto della governance di un ecosistema complesso come Internet è l'identità degli utenti. Saranno ripercorsi i tentativi di approcciare il tema dell'identità online: iniziali soluzioni centralizzate hanno lasciato spazio a proposte federate e le tendenze di democratizzazione e digital sovereignty hanno successivamente permesso il fiorire di un nuovo approccio, quello della *Self Sovereign Identity*. Partendo da una disamina della normativa in vigore in Europa, con alcuni richiami agli interventi regolatori previsti a livello eurounionale, si cercherà di esporre quali strumenti – tecnici e organizzativi – sono più idonei per il raggiungimento di un mercato digitale sicuro e affidabile.

Digital trust – Digital identity – eIDAS

Sommario: *1. Il significato dell'Internet governance – 2. Il ruolo della regolamentazione – 3. Identità digitale e presenza degli utenti in rete – 4. Conclusioni*

To be, or not to be (a part of the networked society):
that is no longer a question but an issue we have to deal with.
C. Costa, R. Torres[1]

1. Il significato dell'Internet governance

L'interazione tra diritto e Internet[2] ha attraversato, sin dalla fine del secolo scorso, diverse fasi: l'oggetto tecnologico, per costituzione indipendente dalla normativa, ha acquisito con il passare del tempo un livello tale di compenetrazione, affidabilità ed essenzialità da chiedersi se una governance specifica non fosse possibile, o perfino necessaria e indispensabile.

In "A Declaration of the Independence of Cyberspace" (1996) John Perry Barlow illustra come il ciberspazio sia un'area senza sovranità, dove una governance non solo non sia auspicabile, ma nemmeno realizzabile. La partecipazione del legislatore nel ciberspazio non è prevista, specialmente in tematiche quali la libertà di espressione, né tantomeno viene riconosciuto il potere esecutivo dello Stato. Il concetto di identità è interpretato come distaccato dalla

I. Marcolongo Head of Business Solutions Compliance, InfoCert – Gruppo Tinexta; L. Piatti, Head of Trust Specialists, Business & Solutions Compliance, InfoCert – Gruppo Tinexta; A. Bossi, Analyst, Business & Solutions Compliance, InfoCert – Gruppo Tinexta

Questo contributo fa parte del numero speciale "La Internet governance e le sfide della trasformazione digitale" curato da Laura Abba, Adriana Lazzaroni e Marina Pietrangelo.

persona fisica, e inteso solo come entità generica che opera in rete.

La proprietà intellettuale, le implicazioni penalistiche e civilistiche delle azioni svolte online, tuttavia, non possono coesistere con l'ideologia di Barlow. I numerosi reati che possono essere commessi in rete, quali hacking, phishing, violazione di copyright, cyberbullismo, distribuzione di materiale pedopornografico, non lasciano dubbi sulla necessità di una regolamentazione *ad hoc*. Anche da un punto di vista civilistico l'ascesa degli e-commerce, la contrattazione telematica, l'erogazione di servizi da remoto e il ruolo dei service provider hanno reso necessario l'intervento del legislatore per garantire un'adozione estesa – e sicura – della nuova tecnologia.

Una visione dell'Internet governance differente rispetto a Barlow è presentata da Lawrence Lessig che con l'espressione "Code is Law" tratta dal libro *Code and Other Laws of Cyberspace* (1999), riprende il concetto di "Lex informatica" coniato da Joel Reidenberg ed esprime la progressiva affermazione del codice come *rule-maker*. Il codice stesso infatti assume un ruolo primario nel regolamentare le interazioni e il comportamento degli utenti di Internet, e della rete stessa[3]. Si assiste, riferendosi a un processo spontaneo e inevitabile che avviene nel ciberspazio, al confluire di un nuovo tassello nella gerarchia delle norme. Nello stesso lavoro, Lessig ammonisce che la libertà nel ciberspazio non sarà data dall'assenza dello Stato, ma da uno Stato che garantisca il controllo di un certo tipo, che favorisca un luogo dove la libertà possa fiorire: si passa dalla visione poetica di Barlow che rifiuta decisamente l'intervento del legislatore, ad una meno radicale in cui viene riconosciuto il ruolo del regolatore, pur mantenendo il codice come un punto di riferimento.

Manifesta attuazione di tale concetto è la nuova era sancita dalla tecnologia blockchain, un particolare tipo di *Decentralized Ledger Technology* ("DLT"), contraddistinto dalla presenza di un codice open-source neutrale, dalla decentralizzazione dell'autorità, dal consenso distribuito e dalla verificabilità delle transazioni che avvengono sul registro pubblico[4]. Tale tecnologia può essere adottata per innumerevoli scopi: oltre alle più conosciute finalità di diffusione di sistemi decentralizzati di pagamento, gestione di criptovalute e attuazione di *smart contracts*, non è da sottovalutare l'accesso a servizi governativi senza limiti territoriali.

La struttura intrinseca della blockchain elimina l'elemento di fiducia tradizionale tra le parti, necessario nelle tipiche e tradizionali interazioni nelle quali un'autorità terza garantisce non solo l'operato dei soggetti, ma la validità delle loro azioni e la sicurezza delle transazioni. La fiducia distribuita che risiede nei nodi si sostituisce alla fiducia derivata da un rapporto contrattuale, rendendo difficile l'individuazione di ruoli e responsabilità negli ecosistemi decentralizzati. A ben vedere, tuttavia, questa componente non è stata eliminata, ma ha permesso la nascita di nuovi intermediari: fornitori di "Blockchain as a service", consulenze su quale Blockchain sia meglio utilizzare, assicurazioni dedicate, etc. Per questo motivo i mercati maggiormente regolamentati stanno utilizzando soluzioni di DLT *permissioned*, in cui – cioè – i verificatori sono noti e l'informazione certificata.

Sebbene il codice sia legge nel ciberspazio, De Filippi e Hassan ci conducono al livello successivo nel quale il diritto si trasforma progressivamente in codice, ossia "Law is Code". L'incorporazione di regole, decisioni e prescrizioni nel codice, quali *smart contracts* o altre disposizioni contrattuali, conferiscono alla blockchain, per la sua natura decentralizzata, il potere di far osservare i vincoli registrati, anche in assenza di una norma legale a supporto. Questo concetto, seppur vero, deve tuttavia tenere in considerazione i limiti tra ciberspazio e mondo reale, nel quale la presenza di un intermediario di fiducia garantisce la possibilità e la funzione di convalidare all'esterno del codice una decisione e di garantirne l'attuazione. Non è inoltre da trascurare la componente interpretativa nell'applicazione di una norma giuridica, resa possibile da prescrizioni generiche che possono adattarsi ad una moltitudine di casi differenti; tale aspetto discorda con la necessità di un codice preciso, specifico, non ambiguo e di immediata attuazione[5].

In definitiva, l'approccio proposto da Lessig e abbracciato – consapevolmente o meno – dai legislatori di tutto il mondo è stato reso necessario per garantire una corretta adozione del Web e delle sue applicazioni: nel paragrafo successivo si cercherà di riportare brevemente gli interventi normativi più rilevanti tesi a proteggere gli utenti e garantire la fiducia nell'ecosistema di Internet. Senza una componente di trust, il mondo digitale sarebbe rimasto il ciberspazio di Barlow: affascinante ma privo delle tutele che oggi permettono ai cittadini di tutto il mondo di utilizzare piattaforme e altre forme di condivisione per scambiarsi valore.

2. Il ruolo della regolamentazione

La regolamentazione assume, nello scenario sopra descritto, un ruolo fondamentale nel delimitare quali siano – *de jure* – gli strumenti con cui il legislatore può garantire che il mercato digitale sia sicuro e, quindi, di facile adozione da parte di tutti i cittadini. Questo paragrafo vuole dare atto della complessa

rete di norme primarie che garantiscono un giusto – e delicato – equilibrio tra usabilità, sicurezza informatica e certezza giuridica.

Tralasciando gli aspetti normativi legati alla sicurezza informatica, e quindi quella branca regolamentare che viene ricondotta sotto la Direttiva NIS (Direttiva sulla sicurezza delle reti e dei sistemi informativi dell'Unione, NISUE 2016/1148)[6], sembra utile concentrarsi sulle Direttive e sui Regolamenti che, negli anni, hanno cercato di costruire fiducia nel mercato digitale. Questo percorso è iniziato nel 1999 con i primi progetti di regolamentazione delle firme elettroniche, e proseguito in modo più formale nel 2015 con il concetto di *Digital Single Market*: il tentativo di creare uno spazio digitale europeo all'interno del quale ciascun cittadino – o più in generale ciascun utente – potesse sfruttare, in un ecosistema tecnicamente sicuro e giuridicamente rilevante, le potenzialità del commercio elettronico. Questa espressione va qui intesa in senso lato: a partire dalle necessità prettamente commerciali di scambio di beni e servizi, a raggiera l'esigenza dell'utente si estende a tutti quegli aspetti della vita quotidiana che abilitano la presenza della singola persona online. Concetti fondamentali di questa "trasformazione digitale" sono l'identità digitale, i documenti e le firme elettroniche, gli strumenti di e-delivery sicuri e con un valore legale certo. L'approccio regolamentare ha tenuto conto non solo degli aspetti squisitamente normativi ma anche di quelli tecnici: tutti i provvedimenti di primo livello sono accompagnati da una normativa di secondo livello che determina un dettaglio tecnologico o – spesso – richiama standard internazionali, come quelli ETSI o ISO.

Già con la Direttiva 1999/93/CE[7], il legislatore europeo aveva fatto un timido tentativo di regolare le transazioni elettroniche e i servizi fiduciari: solo nel 2014, tuttavia, con il Regolamento UE n. 910/2014 (c.d. "eIDAS")[8] – proprio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno – si è venuta a creare una solida base giuridica che ha permesso lo sviluppo di un ecosistema digitale basato su concetti tradizionali di sicurezza e fiducia. In particolare, il Regolamento eIDAS, è diviso in due parti principali: la prima – artt. 6-12 – regola l'identità digitale, la seconda – artt. 13-46 – descrive il funzionamento dei servizi fiduciari. Per quanto riguarda l'identità (o anche "eID"), il legislatore europeo ha creato un ecosistema centralizzato in cui ciascuno Stato membro è tenuto a valutare e verificare la bontà del proprio strumento di identità digitale: attraverso una procedura di notifica ciascuno Stato è in grado di presentare la propria soluzione alla Commissione che – grazie ai propri organi di valutazione e ad un momento di peer-review – decide se lo strumento è sufficientemente sicuro per essere riconosciuto in tutti e 27 gli Stati membri. Questo aspetto è particolarmente importante: il completamento della notifica, infatti, rende lo strumento utilizzabile in ciascuno Stato membro, attraverso un sistema di nodi di intermediazione (proxy) che risolvono le criticità di interoperabilità tecnica. Un'accortezza interessante risiede nel fatto che il legislatore ha previsto tre diversi livelli di sicurezza – "fiducia" – per ciascuna eID: *basso*, *significativo* e *elevato*. Questo approccio, dettato dalle esigenze del mercato, permette di utilizzare una eID a seconda del caso d'uso: non tutti i casi d'uso hanno, infatti, bisogno degli stessi elevati livelli di sicurezza, che spesso hanno come contraltare il sacrificare l'usabilità lato utente. Si immagini, ad esempio, l'uso di una eID nel contesto bancario, dove gli standard di sicurezza sono sicuramente molto alti: sarà richiesto un livello *elevato* o per lo meno *significativo*. Al contrario, per l'accesso alla biblioteca di quartiere potrebbe essere sufficiente un livello *basso*, con una considerevole abbassamento dei costi e migliore utilizzabilità. Come descritto in premessa, esistono dettagli tecnici e funzionali sulle modalità con cui ciascun livello di fiducia può essere raggiunto: la Commissione – con l'Atto di implementazione n. 2015/1502[9] – ha definito tutti i parametri che il medesimo strumento deve rispettare per essere riconosciuto nel corretto *Level of Assurance* ("LoA").

La seconda parte del Regolamento è dedicata ai servizi fiduciari: questa descrive tutti quegli strumenti elettronici che permettono un corretto scambio di informazioni e valore online. Il legislatore si è concentrato sulle firme elettroniche, i sigilli elettronici, la conservazione dei certificati elettronici, le validazioni temporali e gli strumenti di recapito elettronici. Per ciascuna di queste categorie sono previsti due livelli di sicurezza: uno semplice e uno qualificato, fanno eccezione le firme e i sigilli, per cui è previsto un livello intermedio definito come "avanzato". Anche in questo caso, il legislatore ha previsto diversi livelli di "trust" per le singole soluzioni: sono definiti i requisiti dei servizi fiduciari *tout court* e quelli dei servizi fiduciari qualificati. In alcuni casi, come per la firma elettronica, viene anche prevista una classe residuale, o "semplice", che permette di dare consistenza al dettato dell'art. 25 co. 1, per cui «A una firma elettronica non possono essere negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali per il solo motivo della sua forma elettronica o perché non soddisfa i requisiti per firme elettroniche qualificate».

Seppur sia rimesso a ciascuno Stato membro di individuare il valore giuridico e la forza probatoria di ciascuno strumento, l'art. 25 riconosce alla sola fir-

ma elettronica qualificata un valore equipollente alla firma autografa: questo permette di mantenere un altissimo grado di interoperabilità per questo strumento in ciascuno dei 27 Stati membri. Come per la notifica – e quindi il riconoscimento – dell'eID, anche per i servizi fiduciari esiste un complesso ecosistema di validazione: ciascuno Stato membro individua una autorità di vigilanza – in Italia AgID – che gestisce le *trust list*, un elenco di soggetti abilitati all'erogazione dei servizi fiduciari. Il livello "qualificato" si raggiunge solo a seguito di un esito positivo di una procedura di valutazione di specifici soggetti, i *conformity assessment body*, che attraverso audit e verifiche accertano che il prestatore di servizi in questione abbia tutte le caratteristiche per erogare un servizio di livello "qualificato". Questo aspetto non è da sottovalutare: è esattamente grazie a questa rete di accreditamento e controllo che il legislatore è in grado di garantire un alto grado di governance nel framework digitale europeo.

Il Regolamento eIDAS è poi integrato in ciascuno Stato membro da normative di settore che normano tutti gli aspetti non direttamente trattati dalla legge europea: in Italia, questo ruolo è ricoperto dal Codice dell'amministrazione digitale (anche conosciuto come "CAD"[10]) e dalle regole tecniche (o linee guida) che lo completano. Nel nostro caso, vengono regolati sia aspetti che sfuggono al Regolamento europeo – come la PEC o la conservazione a norma – sia aspetti di dettaglio come appunto il valore giuridico e probatorio di ciascuno strumento. Questo aspetto tende a indebolire la portata di governance generale del Regolamento, ma è un approccio necessario per evitare che l'armonizzazione tecnologica europea porti eccessivo squilibrio negli ordinamenti di ciascuno Stato membro: il bilanciamento trovato dal legislatore ha permesso negli anni di aumentare la fiducia nei servizi digitali.

Il Regolamento eIDAS risale al 2014, è in corso un'operazione di aggiornamento che comprende non solo la rimodulazione di strumenti già presenti, ma anche l'inserimento di nuovi servizi fiduciari: seppur si tratti di una prima proposta, soggetta probabilmente a future modifiche, possono già essere individuati alcuni punti di interesse.

Tra questi emergono nuovi servizi fiduciari, quali servizi di conservazione elettronica qualificata, registri elettronici, l'*European digital identity wallet* e gli attestati di attributi elettronici. Questi ultimi due sono particolarmente rilevanti per il percorso che stiamo cercando di fare con il presente articolo: si tratta di strumenti tecnologici già utilizzati da diversi anni, ma privi di un vero e proprio trust framework. A questo si aggiungono i registri elettronici: la gestione di database o ledger è destinata a diventare un servizio fiduciario. La somma di tutte queste variabili è un chiaro segnale che il legislatore sta cercando di addentrarsi nel nuovo Internet, quello delle DLT cui si faceva riferimento poco sopra, caratterizzato dalla decentralizzazione e da nuovi protagonisti che non sempre sono facilmente individuabili.

Regolare gli strumenti utilizzati, tuttavia, non è attività sufficiente per garantire una governance solida e creare un ecosistema di fiducia tale da permettere l'adozione estesa delle nuove tecnologie: il legislatore, infatti, ha previsto un'articolata disciplina degli acquisti online, improntata per lo più alla protezione del consumatore. Nel 2000 con la Direttiva sul commercio elettronico (Direttiva 2000/31/CE)[11], insieme al suo recepimento in Italia con il D.lgs. 70/2003[12], vengono regolati tutti quegli aspetti che attengono ai "servizi della società dell'informazione". In particolare, vengono descritte le modalità di conclusione dei contratti online (o telematici), compreso il dettaglio delle clausole vessatorie, gli obblighi informativi verso gli utenti, nonché le sanzioni previste per i prestatori di servizi. Questo punto è particolarmente importante, perché riflette la serietà del legislatore nel creare una cornice chiara e sicura all'interno della quale gli utenti possano acquistare e scambiare valore. Il concetto di acquisto da remoto può sembrare scontato a 20 anni di distanza, ma in quella sede il legislatore ha dovuto bilanciare gli interessi imprenditoriali con i diritti di soggetti in qualche modo "fragili": l'asimmetria informativa è stata la ragione principale dell'incapacità dell'utente di muovere passi sicuri nella contrattazione telematica, che il regolatore ha cercato di compensare imponendo ai prestatori di servizi oneri informativi e sanzioni di diverso grado, nonché ampi diritti a favore dei consumatori (si pensi al recesso *ad nutum* entro i 14 giorni dall'acquisto).

Anche la regolamentazione del contesto finanziario ha fortemente contribuito alla governance della rete, diventando nel tempo uno standard *de facto* e un *driver* per l'evoluzione tecnologica: le varie Direttive *Anti Money Laundering* ("AML") – e i rispettivi provvedimenti di ricezione, che si trovano all'interno del d.lgs. n. 231/2007[13] – hanno permesso la nascita e lo sviluppo di piattaforme bancarie online. In particolare, gli articoli dedicati al riconoscimento della clientela da remoto, hanno abilitato processi di *onboarding* digitali, altrimenti non praticabili. Inoltre, la Direttiva (EU) 2015/2366 sui *payment services* ("PSD2")[14] ha rafforzato la fiducia nelle transazioni, imponendo l'utilizzo di strumenti di digital trust, quali l'autenticazione a due fattori e l'autenticazione sicura tra server (QWAC), oltre a importanti

aspetti legati all'open banking: questo ha indubbiamente portato gli utenti ad approcciare con più serenità processi remoti e innovativi, in un contesto così delicato come quello dei pagamenti elettronici.

Un importante strumento di interconnessione tra le numerose normative sopra citate è il Regolamento Generale sulla Protezione dei Dati Personali ("GDPR")[15]: con questo intervento, come noto, il legislatore europeo ha rafforzato la tutela dei dati personali, sostituendo la precedente Direttiva 95/46/CE. Questo strumento è stato previsto sia per tutelare i dati dei cittadini – e quindi degli utenti – sia per garantire ai prestatori di servizi e agli Stati sovrani uno strumento in grado di assicurare un trattamento legittimo dei dati. Questo è un aspetto assolutamente rilevante per la governance del Web: il regolatore non si è limitato a creare uno strumento protettivo per gli interessati, ma si è spinto sino a cercare forme per cui i dati potessero essere utilizzati da quei titolari che – per motivi di opportunità o business – ne traessero utilità per i diversi scopi di business. Al netto dei recenti tentativi – si veda ad esempio la Direttiva 770/2019[16], relativa a determinati aspetti dei contratti di fornitura di contenuto digitale e di servizi digitali – di monetizzazione dei dati, che non sempre incontrano il favore del Garante per la protezione dei dati personali, è prevista una complessa architettura di consensi ed eccezioni per permettere un uso trasparente e legittimo dei dati. Questo aspetto si inserisce in maniera trasversale rispetto a tutte le normative sopra citate, in quanto da una parte la protezione dei dati è sempre richiamata formalmente, dall'altra un corretto trattamento dei dati è essenziale proprio per poter offrire servizi digitali, che – fondamentalmente – vengono alimentati proprio dai dati personali.

A sottolineare l'importanza dei dati nell'epoca dell'informazione, c'è anche il Regolamento (UE) 2018/1807[17], in materia di protezione dei dati non personali: la cura anche di questi aspetti permette di garantire al mercato unico digitale un trasferimento, trattamento e scambio di dati sicuro, alimentando così la transizione digitale.

Il legislatore si sta impegnando, inoltre, ad aggiornare l'intero impianto normativo: con due importanti proposte, il *Digital Services Act*[18] e il *Digital Markets Act*[19], intende definire un quadro giuridico idoneo alle tecnologie moderne che garantisca la sicurezza degli utenti online, stabilendo una governance con la protezione dei diritti, mantenendo allo stesso tempo appetibile la "Platform economy" per tutti gli attori nazionali e internazionali.

3. Identità digitale e presenza degli utenti in rete

L'evoluzione di Internet, l'incremento degli strumenti che la rete mette a disposizione e lo sviluppo di innumerevoli applicazioni Web hanno inevitabilmente influito, e continuano a incidere, sulla presenza degli utenti in rete. In un primo momento si assiste alla creazione di pagine Web statiche rivolte ai consumatori come strumento di sola lettura, adatte per fornire informazioni e strumenti con un approccio *top-down*, in particolar modo a livello istituzionale e ad opera di fornitori di servizi. Si è in seguito verificato il passaggio a quello che viene definito "Web 2.0", con una partecipazione attiva degli utenti e con possibilità di accesso e creazione di contenuti. La scoperta dei molteplici livelli di Internet, e la conseguente presenza interattiva degli utenti online, hanno inoltre introdotto per molti web-users il cambiamento della condizione di anonimato in volontà di coltivare un'identità online. La corsa alla creazione di spazi personali sul Web, come blog o profili su diversi social network, la propensione a geolocalizzarsi rendendo noti i luoghi frequentati, la partecipazione a discussioni in rete e l'integrazione di profili professionali hanno assecondato lo spirito di condivisione di molti internauti. Con l'aumentare delle informazioni diffuse sul Web, tuttavia, è cresciuta anche la consapevolezza degli utenti rispetto a ciò che stavano condividendo, le azioni che stavano compiendo, la loro effettiva presenza in rete e le implicazioni che queste attività hanno nel mondo offline. Questa cognizione, unita alla crescente attenzione del legislatore a disciplinare la materia come illustrato nel precedente paragrafo, ha portato molti utenti a vagliare il proprio comportamento online. L'iniziale frenesia di condivisione ha lasciato il passo alla moderata valutazione e, per alcuni, anche alla ricerca dell'anonimato. Conservare o raggiungere questa condizione, tuttavia, non è un fine che tutti gli utilizzatori desiderano perseguire, soprattutto se all'utente stesso sono forniti gli strumenti previsti dalla normativa atti a tutelare e gestire l'identità digitale e i propri dati personali. Emerge quindi il vero obiettivo: esercitare un controllo progressivo sulla propria individualità e sulle informazioni condivise nel corso del tempo su Internet[20].

Le prime forme di riconoscimento degli utenti in rete sono state scandite dalla scelta di username, in seguito arricchito da una password, abitualmente collegate ad un indirizzo e-mail, atte a creare profili digitali che permettessero all'utente di interagire con il servizio o la pagina Web di riferimento. Il proliferare di molteplici utenze diverse ha permesso al modello così detto "federato" di farsi strada. In rela-

zione a questo modello, l'identità è gestita da un solo service provider che mette a disposizione dell'utente il sistema di autenticazione centralizzato, userID e password, il quale permette di autenticarsi presso fornitori ulteriori rispetto al provider che ha creato l'identità, secondo un framework di fiducia tra i provider (*federation*). L'utente pertanto non deve ottenere dati di autenticazione per ogni servizio o creare un account per ogni prestazione online, ma con una sola autenticazione può identificarsi e accedere a servizi di diversi fornitori. La *user experience* di questo modello è certamente molto positiva; tuttavia, alcune criticità rispetto alla delegazione dell'identificazione in capo ad un unico soggetto possono essere individuate. Ad esempio, la gestione delle informazioni condivise dall'utente nel tempo, l'esercizio dei diritti dell'interessato in un'ottica di protezione dei dati personali ed eventuali rischi di sicurezza delle informazioni.

L'incremento della partecipazione online, la digitalizzazione di numerosi servizi – essenziali e non – e le nuove opportunità nate dall'economia digitale, hanno portato alla necessità di identificare gli utenti in rete in modo univoco, e in molti casi, all'esigenza di associare l'identità digitale ad un'identità fisica offline. Per garantire non solo questo collegamento, ma anche la sicurezza informatica dei dati e delle informazioni trattate e per evitare il delinearsi di diverse soluzioni frammentate, si è prospettato un modello basato sul concetto di identità decentralizzata. Questo framework si serve della crittografia e di una struttura decentralizzata, quale quella abilitata dalle *Decentralized Ledger Technologies* (DLT), di cui la Blockchain fa parte, per consentire all'utente di creare identità digitali decentralizzate sicure, che rimangano sotto la sua amministrazione e il suo costante controllo. Soluzioni crittografiche fornite da prestatori di servizi fiduciari qualificati quali la firma elettronica qualificata per la persona fisica, e i sigilli elettronici per le persone giuridiche, possono permettere agli utenti di attuare il collegamento con la propria identità offline e di ottenere credenziali verificabili (*verifiable credentials* VCs) a supporto di tale connessione.

Un approccio all'identità digitale decentralizzata, noto come *Self-Sovereign Identity* (SSI), permette al titolare di gestire, oltre alla propria identità digitale, ulteriori dati ad essa collegati; l'utente può infatti selezionare in modo attivo, ogni volta che un'identificazione si renderà necessaria, quali dati nello specifico condividere con il destinatario e mantenere la sua regolare supervisione su di essi[21]. Tale metodo permette di gestire il consenso, o la revoca dello stesso ai fini di trattamenti di dati personali, di assicurare il rispetto dei principi di minimizzazione e trasparenza e di garantire l'esercizio dei diritti dell'interessato in termini di accesso e portabilità.

La mancanza di fiducia, spesso effettiva nel mondo digitale, dovuta alla presenza di connessioni e scambi con soggetti dei quali non si ha modo di conoscere la vera identità, alla necessità di dover rivelare senza controllo informazioni, nonché alla difficoltà di dimostrare la provenienza di dati ricevuti, ha portato alla creazione di un progetto noto come "Trust Over IP" (TOIP) che nel 2020 ha assunto lo status di fondazione[22]. L'obiettivo di quest'ultima è ripristinare l'elemento fiduciario colmando il "trust gap" tra i diversi attori online con i seguenti strumenti, e non solo: l'accertamento di identità e attributi verificati, l'uso di *wallet* digitali interoperabili e l'adozione di standard globali per connessioni private. Tali concetti sono da tempo sostenuti da Drummond Reed, co-fondatore di TOIP Foundation e grande teorico dei temi di identità distribuita. Egli infatti già nel 2017 aveva dichiarato che le SSI fossero «il culmine naturale dell'evoluzione dell'identità in Internet, allora consegnarla richiede fiducia diffusa, portabilità, sicurezza e nessun singolo punto di fallimento o controllo» e la DLT risulta l'unico meccanismo sicuro per raggiungere tale obiettivo[23].

Dal punto di vista della normativa, come già indicato, il Regolamento eIDAS prescrive il riconoscimento reciproco all'interno dell'Unione europea tra regimi di identificazione elettronica, sia per le persone fisiche che per le persone giuridiche, e detta le modalità di notifica dei regimi stessi. L'evoluzione con il testo proposto per eIDAS 2.0[24] è nella presentazione di una soluzione di identità digitale sicura e affidabile riconosciuta tra gli Stati membri che amplifichi le funzioni dei documenti nazionali elettronici e che conduca all'affermazione di un'identità nel pieno controllo del suo titolare[25].

Sicurezza delle persone, sicurezza dei dati, facilità d'uso, accessibilità a servizi pubblici e privati, affidabilità, inclusività e interoperabilità sono solo alcuni dei punti cardine alla base dell'introduzione dell'identità digitale europea. Ogni Stato membro dovrà dotarsi di infrastrutture per emettere Portafogli europei di identità digitale (*European digital identity wallets*, nel prosieguo "wallet") con conseguenti costi amministrativi e finanziari che saranno tuttavia ripagati dai benefici che un'armonizzazione giuridica porterà a tutti gli utenti. Ogni prestatore di servizi, pubblico e privato, per la cui prestazione è richiesta un'autenticazione forte potrà garantire l'accesso e l'identificazione tramite soluzioni che siano in grado di dialogare con lo standard su cui i *wallet* sono costruiti. In particolare, in un contesto rispettoso

del paradigma SSI, ciascun utente potrà spendere le proprie VC attraverso il *wallet* al fine di dimostrare la propria identità o un attributo relativo alla propria sfera personale. Interessante notare come le azioni di autenticazione e identificazione garantite da questi oggetti possano essere effettuate anche offline, per rispondere ad esigenze di alcuni settori basati principalmente sull'interazione fisica, quale il settore sanitario. Per ottenere questa interoperabilità è ancora una volta fondamentale l'intervento del legislatore: ci si aspetta che con eIDAS 2.0 – come sopra descritto – si possa ottenere una soluzione unica per tutta l'Europa.

Numerosi aspetti dell'approccio SSI saranno implementati nel *wallet*, in modo da garantire che il titolare dell'identità digitale abbia a disposizione gli strumenti adatti per selezionare quali informazioni, attributi, qualifiche o credenziali condividere digitalmente in sicurezza. Questo approccio permette di rispettare i principi sanciti dal GDPR, quali il controllo del dato e la minimizzazione del trattamento, e rende particolarmente fluidi processi di raccolta e spendita del consenso al trattamento.

Da una gestione totalmente centralizzata dell'identità, tipica del Web 2.0, si è quindi transitati verso modelli frammentati, creati dall'utente ma la cui gestione rimaneva strutturalmente associata al proprietario della piattaforma di riferimento, per arrivare, con il Web 3.0, a modelli di identità digitale decentralizzata. Grazie al paradigma SSI, tali modelli garantiscono non solo la lettura e la scrittura, ma permettono di esercitare concretamente il controllo della e sulla propria identità. Venendo meno la centralizzazione, tutte le informazioni sono in capo e a disposizione del titolare, il quale tramite un *wallet* installato sul proprio cellulare potrà anche gestire certificati di proprietà e oggetti digitali quali NFT[26]. L'identità dell'utente in rete si apre, si confronta con l'identità reale del soggetto e non ne è distinta.

Uno strumento strettamente collegato all'identità digitale è il domicilio digitale, previsto dall'art. 3-*bis* del CAD per ricevere comunicazioni elettroniche aventi valore legale. Per eleggere il domicilio digitale è necessario essere in possesso di un recapito elettronico certificato o certificato qualificato. Ad oggi in Italia la designazione è possibile tramite il servizio di posta elettronica certificata e un'apposita procedura formale di elezione, che tuttavia non garantisce di per sé l'identità certa del titolare della casella. Tramite la creazione e consultazione di elenchi di corrispondenza tra domicili digitali e imprese, professionisti e cittadini è possibile avere a disposizione l'indirizzo PEC fornito dall'impresa, professionista o cittadino corrispondente. Dal 2013 con l'istituzione da parte del Ministero dello Sviluppo Economico di INI-PEC si è reso obbligatorio per imprese e professionisti iscritti in albi o registri eleggere un domicilio digitale. Si tratta di un elenco regolarmente aggiornato e consultabile da parte di tutti gli utenti senza necessità di autenticazione. Con la Determinazione n. 529/2021 AGID ha inoltre dato l'avvio a INAD, l'Indice dei domicili digitali che raccoglierà i domicili digitali volontariamente eletti da parte di persone fisiche, professionisti e altri soggetti non sottoposti all'obbligo di cui sopra. Prima di eleggere il domicilio digitale sarà necessaria una fase di identificazione univoca, tramite SPID, CIE o CNS. I domicili digitali eletti dalle persone fisiche saranno inoltre trasmessi quotidianamente all'ANPR (Anagrafe Nazionale Popolazione Residente) che raccoglie i dati anagrafici dei cittadini in modo da assicurare la consistenza delle informazioni alla base dei procedimenti di tutti gli enti della pubblica amministrazione. Questo percorso è strategico per la digitalizzazione della PA tanto auspicata in questi anni, ma comporta una serie di criticità stante la varietà di situazioni da regolare. Ad esempio, il Garante per la protezione dei dati personali ha sottolineato alcune problematiche in merito alla possibilità di utilizzare gli indirizzi PEC presenti in INI-PEC per l'invio di comunicazioni aventi valore legale[27]. Accade, infatti, che numerosi indirizzi PEC professionali di ordini o collegi siano gestiti non soltanto dal diretto titolare, ma anche da parte di collaboratori e colleghi, venendo quindi a mancare la riservatezza delle comunicazioni stesse. Tale è il caso della ricezione di verbali di accertamento per infrazioni del codice della strada, tema sul quale il Garante ha recentemente ribadito la sua posizione[28] escludendo la possibilità di inviare questo tipo di comunicazioni al domicilio digitale professionale. Per ovviare al problema il professionista iscritto nell'INI-PEC potrà registrarsi all'INAD in qualità di persona fisica, in modo da poter separare le comunicazioni di competenza lavorativa da quelle appartenenti alla sfera privata. Allo stesso modo, per garantire la divisione di questi due ambiti, all'interno dell'INAD sarà prevista la possibilità per i professionisti non presenti in INI-PEC di eleggere un domicilio digitale professionale, e uno personale, entrambi riferiti al medesimo soggetto. Sia a livello nazionale[29], che europeo[30], l'obiettivo è implementare le piattaforme per proporre recapiti elettronici certificati qualificati, in modo da garantire *ex ante* l'identità certa del titolare del recapito elettronico, e dipanare ogni dubbio in merito al tema della gestione del conseguente domicilio digitale eletto.

Per l'utente della rete si evince quindi sempre più la necessità di disporre di strumenti adeguati atti

a garantire il controllo sulle proprie informazioni, a permettere la gestione efficiente delle comunicazioni digitali, e a consentire l'esercizio dei diritti previsti dalle normative vigenti. Tali strumenti devono poter tenere in considerazione la dinamicità e la complessità del contesto digitale in cui sono declinati, e allo stesso modo saper sfruttare le opportunità che il framework di riferimento offre. Questo concerne tutti i diritti che concorrono alla macrocategoria di "diritto alla privacy" che annovera al suo interno distinti diritti quali il diritto alla protezione dei dati personali, alla reputazione, all'auto-determinazione e, non da ultimo, all'identità[31].

Il diritto all'identità, e il diritto all'identità digitale, sono parti della sfera personale dell'individuo, concorrono alla sua autodeterminazione e alla sua autonomia verso un modello di cittadinanza digitale consapevole, responsabile e affidabile. Sullivan ritiene fondamentale il riconoscimento e la protezione del diritto all'identità digitale, tema che frequentemente, ed erroneamente, viene messo in secondo piano rispetto alla protezione dei dati personali. In egual modo infatti questi diritti, ognuno secondo le proprie peculiarità, contribuiscono all'affermazione dell'individuo e si differenziano nella relazione con l'interesse pubblico[32]. Come difatti confermato dal GDPR[33], l'interesse pubblico in molteplici contesti sovrasta il diritto alla protezione dei dati personali, al contrario rispetto al diritto all'identità che non è subordinato a, o condizionato da, motivi di interesse pubblico.

Tale concetto è inoltre esposto ed affermato nell'art. 8 della Convenzione europea dei diritti dell'uomo[34]: ogni individuo ha diritto al rispetto della propria vita privata e familiare, e ogni forma di ingerenza pubblica deve essere giustificata dalla legge o da un interesse di grado superiore e collettivo.

Si potrebbe raffigurare l'identità digitale come composta da due set di informazioni: una prima parte riguarda dati statici, che indicativamente non si modificano con il passare del tempo, quali i dati anagrafici, e una seconda categoria di informazioni che si aggiornano periodicamente. Interessante notare come la prima tipologia consti di dati ampiamente reperibili in registri pubblici e quindi ipoteticamente meno tutelati giuridicamente sotto il profilo di protezione dei dati personali. Tali dati devono tuttavia essere protetti in quanto sono il punto di accesso per il secondo insieme di informazioni[35] che riguardano l'individuo, quali dati medico-sanitari, diplomi di istruzione o informazioni finanziarie.

Gli strumenti che abilitano l'identità digitale hanno quindi una duplice valenza, da un lato garantire e portare all'autodeterminazione dell'utente, come strumento di affermazione di individualità e controllo sui propri dati, dall'altro sono mezzi di cui avvalersi in relazione ai rapporti con lo Stato, che richiede informazioni certe per esercitare la propria governance.

4. Conclusioni

Siamo in un momento storico e sociale in cui Internet ha raggiunto una relazione molto intima con gli utenti: da una prima diffusione, che possiamo temporalmente collocare nell'ultimo decennio del Novecento, si è passati velocemente negli ultimi vent'anni a una fase in cui la rete e i servizi online sono progressivamente diventati via via più pervasivi nella vita degli utenti. Oggi ci troviamo in una situazione di quasi dipendenza di Internet: non solo i servizi critici, come quelli governativi o di difesa, non possono fare a meno della rete, ma anche i servizi essenziali, come quelli legati alla salute o all'istruzione, risultano di difficile utilizzo in assenza di una connessione. In questo contesto sembra ancora più necessaria una presa di posizione ferma da parte del regolatore, un sistema di governance che sia attuale e possa essere efficacemente utilizzato per gestire le nuove tecnologie del web: intelligenza artificiale, Internet of Things e DLT.

Il *Digital Market Act* ("DMA") è un ottimo esempio di questa tendenza: la qualificazione delle grandi piattaforme online quali "gatekeepers" (controllori dell'accesso) testimonia l'attenzione del legislatore alla creazione di un ecosistema controllato in cui l'utente possa autodeterminarsi senza temere la lesione dei propri diritti e senza delegare eccessivamente ai privati queste importanti attività. Il DMA, infatti, sancisce per i gatekeepers una nuova serie di obblighi che precludono l'attuazione di pratiche sleali avvalendosi della loro posizione predominante e consolidata nel mercato. Ai sensi del proposto art. 2, come "servizio di piattaforma di base" si individuano ad esempio: motori di ricerca online (come Google), servizi di social network online (Facebook), servizi di piattaforme per la condivisione di video (ad esempio YouTube), servizi di comunicazione elettronica interpersonale indipendente dal numero (ad esempio WhatsApp). L'obiettivo è garantire una concorrenza equa per tutti i fornitori di servizi digitali, accompagnata dall'incremento dell'innovazione, con una forte attenzione verso la protezione dei consumatori e, conseguentemente, dei loro dati personali.

eIDAS è stata la prima normativa che ha cercato di portare uniformità tecnologica all'interno del mercato europeo: la descrizione di diverse soluzioni, dall'identità digitale alla firma, per garantire uno scambio sicuro di informazioni e l'interazione tra cittadini e piattaforme, ha favorito la nascita di un trust *de facto* nei rapporti digitali. Gli utenti, le istituzioni e

le imprese sono confidenti nell'utilizzare le nuove tecnologie anche in rapporti complessi o che coinvolgono patrimoni ingenti. Per raggiungere questo obiettivo, il legislatore europeo non si è limitato a far un riferimento univoco a soluzioni tecnologiche ma ha creato un concetto di governance complesso, composto da una parte dai prestatori di servizi specifici – i prestatori di servizi fiduciari, anche qualificati – e dall'altra da enti di sorveglianza e accreditamento: in questo modo si è creato un ecosistema di fiducia digitale data dai costanti controlli e verifiche effettuati dai secondi nei confronti dei primi.

Tuttavia, la normativa che per quasi dieci anni ha guidato utenti e aziende verso la fiducia nel mondo digitale, ha inevitabilmente perso efficacia verso le più nuove tecnologie e le ultime logiche di interazione tra utenti, istituzioni e attori commerciali. È auspicabile che il nuovo Regolamento eIDAS, e l'evoluzione delle normative sopra richiamate (par. 2), prenda in considerazione da una parte il mutato scenario tecnologico e sociale – come, ad esempio, l'inclinazione del consumatore per il digitale oppure l'avvento di Intelligenza Artificiale, IoT e DLT – dall'altra non vengano dimenticati i limiti che l'attuale regolamentazione possiede, in modo da sfruttare il momento di aggiornamento per superarli. Su questo secondo punto si pensi ad esempio ad un approccio eccessivamente centralizzato, alla mancanza di uniformità giuridica delle soluzioni tecnologiche oppure ancora alla rigidità di determinati processi.

Come Internet e il Web sono nati da strumenti squisitamente tecnologici per poi essere regolamentati in modo da creare fiducia nel digitale e quindi adozione di massa, così le nuove tecnologie richiedono la presenza di ecosistemi di trust ben definiti, che possano garantire una continuità di utilizzo da parte degli utenti: trust framework dedicati che definiscano attori, ruoli e responsabilità. Questo approccio non solo garantisce il rispetto dei diritti ma abilita un mercato digitale cui il nostro Paese non può sottrarsi.

Note

[1] C. Costa, R. Torres, *To be or not to be, the importance of Digital Identity in the networked society*, in "Educação, Formação & Tecnologias", April 2011, p. 51.

[2] Una premessa semantica: seppur Internet e Web siano due concetti ben diversi, il primo un'infrastruttura e il secondo un software, in questo articolo saranno usati con il medesimo significato. Internet e Web come ecosistema, come luogo digitale in cui diversi attori interagiscono tra loro.

[3] P. De Filippi, S. Hassan, *Blockchain technology as a regulatory technology: From code is law to law is code*, in "First Monday", vol. 21, 2016, n. 12.

[4] M. Atzori, *Tecnologia blockchain e governance decentralizzata: lo Stato è ancora necessario?*, disponibile in SSRN, 1° dicembre 2015, p. 7.

[5] P. De Filippi, S. Hassan, *op. cit.*, pp. 15, 17.

[6] Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.

[7] Direttiva 1999/93/CE del Parlamento europeo e del Consiglio, del 13 dicembre 1999, relativa ad un quadro comunitario per le firme elettroniche.

[8] Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE.

[9] 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.

[10] Decreto legislativo 7 marzo 2005, n. 82 *Codice dell'amministrazione digitale* c.d. CAD.

[11] Direttiva 2000/31/CE del Parlamento europeo e del Consiglio, dell'8 giugno 2000, relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno («Direttiva sul commercio elettronico»).

[12] Decreto legislativo 9 aprile 2003, n. 70, *Attuazione della direttiva 2000/31/CE relativa a taluni aspetti giuridici dei servizi della società dell'informazione nel mercato interno, con particolare riferimento al commercio elettronico.*

[13] Decreto legislativo 21 novembre 2007, n. 231, *Attuazione della direttiva 2005/60/CE concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo nonché della direttiva 2006/70/CE che ne reca misure di esecuzione.*

[14] Direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio, del 25 novembre 2015, relativa ai servizi di pagamento nel mercato interno, che modifica le direttive 2002/65/CE, 2009/110/CE e 2013/36/UE e il regolamento (UE) n. 1093/2010, e abroga la direttiva 2007/64/CE.

[15] Regolamento (UE) 2016/679 del Parlamento europeo 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).

[16] Direttiva (UE) 2019/770 del Parlamento europeo e del Consiglio, del 20 maggio 2019, relativa a determinati aspetti dei contratti di fornitura di contenuto digitale e di servizi digitali.

[17] Regolamento (UE) 2018/1807 del Parlamento europeo e del Consiglio, del 14 novembre 2018, relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea.

[18] Proposta di Regolamento del Parlamento Europeo e del Consiglio relativo a un mercato unico dei servizi digitali (legge sui servizi digitali) e che modifica la direttiva 2000/31/CE, 2020/0361 (COD).

[19] Proposta di Regolamento del Parlamento Europeo e del Consiglio relativo a mercati equi e contendibili nel settore digitale (legge sui mercati digitali) 2020/0374 (COD).

[20] *Ivi*, pp. 47-49.

[21] T. Lyons, L. Courcelas, K. Timsit, *Blockchain and Digital Identity. A thematic report prepared by the European Union Blockchain Observatory & Forum*, Blockchain for Government and Public Services, 2 May 2019.

[22] *Introducing the Trust over IP Foundation*, 5 May 2020.

[23] A. Tobin, D. Reed, *The Inevitable Rise of Self-Sovereign Identity. A white paper from the Sovrin Foundation*, 28 March 2017, p. 12, «if self-sovereign identity is the natural culmination of the evolution of Internet identity, then delivering it requires diffuse trust, portability, security and no single point of failure or control. Cryptographically secure distributed ledger technology provides the mechanism to make that happen».

[24] Proposta di Regolamento del Parlamento Europeo e del Consiglio che modifica il regolamento (UE) n. 910/2014 per quanto riguarda l'istituzione di un quadro per un'identità digitale europea, COM/2021/281.

[25] European Commission – eIDAS Observatory, *eIDAS supported Self-Sovereign Identities*, May 2019.

[26] *Non Fungibile Token*, asset digitale intangibile e non fungibile realizzato con tecnologia crittografica che permette di certificare la proprietà di un ulteriore oggetto digitale, come ad esempio un'opera d'arte o un avatar in un ecosistema virtuale.

[27] Garante per la Protezione dei Dati Personali, *Parere all'AgID sullo schema di Linee guida dell'Indice nazionale dei domicili digitali delle persone fisiche, dei professionisti e degli altri enti di diritto privato non tenuti all'iscrizione in albi, elenchi o registri professionali o nel registro delle imprese*, 22 luglio 2021.

[28] Circolare Ministero dell'Interno n. 300-STRAD-1-10060. U-2021 del 17 novembre 2021, nota n. DRP/PS/147434 del 27 ottobre 2021.

[29] AgID, *Servizi di recapito certificato qualificato eIDAS*, 14 giugno 2021 e Id., *PEC: verso i servizi di recapito certificato qualificato*, 16 luglio 2021.

[30] Art. 44 eIDAS.

[31] S. Wachter, B. Mittelstadt, *A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI*, in "Columbia Business Law Review", 2019, n. 2, p. 125.

[32] C. Sullivan, *Digital Citizenship and the Right to Digital Identity Under International Law*, in S. Kierkegaard (ed.), "Information Ethics and Security", 2014, p. 72-84, disponibile in SSRN.

[33] A fini di archiviazione nel pubblico interesse, o di ricerca scientifica o storica o a fini statistici (50), nel settore del diritto del lavoro e della protezione sociale e per finalità di sicurezza sanitaria (52), per finalità connesse alla salute (53), nel settore della sanità pubblica (54), fini di associazioni religiose ufficialmente riconosciute (55), nel corso di attività elettorali (56), per imporre limitazioni a specifici principi e diritti ove ciò sia necessario e proporzionato per la tutela di altri importanti obiettivi di interesse pubblico generale dell'Unione o di uno Stato membro, per la tenuta di registri pubblici per ragioni di interesse pubblico generale (73), per trasferire dati se sussistono motivi di rilevante interesse pubblico (111), l'accesso del pubblico ai documenti ufficiali (154 e art. 86), l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri (art. 6 lett. e), il trattamento di categorie particolari di dati personali (art. 9 lett. g e i), opposizione al diritto alla cancellazione (art. 17 co. 3 lett. c), deroga alla limitazione del trattamento (art. 18 co. 2), deroga al diritto di opposizione (art. 21 co. 6), limitare la portata di obblighi e diritti (art. 23 co. 1 lett. e), deroghe in specifiche situazioni (art. 49 co. 1 lett. d e co. 5).

[34] *Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali*, Roma, 4 novembre 1950.

[35] C. Sullivan, *op. cit.*

* * *

Internet governance: a digital trust matter

Abstract: There are two fundamental pillars that today grant a strong Internet with a reliable and globally usable governance: regulation and digital identity. The evolution of the Internet will be described starting from these two enablers of digital trust. Under the first aspect, initially the meaning and impact that Internet Governance has had at a theoretical-philosophical level will be analysed, investigating the relationship between law and code, and subsequently it will be examined in concrete terms what has been carried out by Italian and European legislators, who have long been looking for the best regulatory formula to guarantee an ecosystem capable of balancing the interests of citizens and the market. The second aspect of governance in an ecosystem as complex as the Internet is user identity. Attempts to approach the issue of online identity will be retraced: initial centralised solutions have given way to federated proposals, and trends towards democratisation and digital sovereignty have subsequently allowed a new approach, the one of Self Sovereign Identity, to flourish. Starting from an examination of the legislation in force in Europe, with some references to the regulatory interventions envisaged at EU level, it will be sought to explain which tools - technical and organisational - are most suitable for achieving a secure and reliable digital market.

Keywords: Digital trust – Digital identity – eIDAS