GIURIMETRICA

RIVISTA DI DIRITTO, BANCA E FINANZA

ANNO 6
NUMERO 1
GENNAIO/GIUGNO
2022

ISSN 2785-2547

almaiura
A VIA PER VIA

RICCARDO GENGHINI*

European identity wallets: Diritti civili e privacy[1]

SOMMARIO: 1. Identità vs. Profilo - 2. Dall'identità come status symbol all'identità come onere sociale - 3. Il mito dell'identificazione come un atto puramente tecnocratico e "neutro" a confronto con la realtà: si tratta di un processo che ha un immediato impatto sui nostri diritti, soprattutto nel contesto digitale - 4. I Wallet come strumento di protezione dell'identità personale e di volontaria presentazione dei propri attributi - 5. Opportunità e rischi del Wallet: come disciplinarlo e implementarlo correttamente - 6. Conclusioni: l'identità (digitale) non può essere una mera finzione giuridica ed occorre che ce ne riappropriamo con la consapevolezza della sua enorme importanza

1. *Identità vs. Profilo* - La proprietà è l'istituto giuridico più antico che si conosca. Ulpiano scrive che il diritto "*tratta di come una cosa diventi di uno, e del come conservi la sua cosa, o del come uno la alieni o la perda*"[2].

All'interno del mondo digitale la proprietà non esiste. La cosa più simile alla proprietà è un dominio informatico chiuso all'interno di un firewall. Non sembra che esistano più domini informatici completamente chiusi in sé stessi: se esistono sono presumibilmente sistemi che debbono garantire il proprio funzionamento ad ogni costo, come piace pensare che siano i *pace makers*, o i sistemi delle centrali elettriche e nucleari. Ma laddove esistano, non si può parlare di proprietà, perché essi sono e funzionano soli ed isolati come Adamo nell'Eden o, meglio, come i primi (personal) computer in stand alone[3].

Se il primo lego-block degli ordinamenti giuridici sono stati il possesso e la proprietà, che nel mondo informatico non hanno un equivalente, quale è la categoria concettuale primigenia nei sistemi informatici?

---

* Notaio in Milano e già Professore di Diritto Commerciale Comparato della Facoltà di Lettere e Scienze Linguistiche dell'Università Cattolica di Milano.

[1] Il presente contributo è una rielaborazione di due precedenti miei scritti: del Capitolo 8.1.4 del mio *Digital New Deal: The Quest of a Natural Law in a Digital Society*, Wolters Kluwer, New York, Amsterdam, Milano 2021 e di *Identità e profilo: il pericolo di confonderli nella società dell'informazion*e, in *Rivista elettronica di diritto economia management*, 2021/1, www.clioedu.it.

[2] D.1.3.41, Ulpiani Institutionorum Libri II.

[3] Per una disamina breve dell'evoluzione del diritto dalla società dei cacciatori nomadi al diritto di una società globalizzata e informatizzata, si rinvia al Capitolo 5 di R. GENGHINI, *Digital New Deal: The Quest of a Natural Law in a Digital Society*.

È l'identità: ogni risorsa in un sistema informatico ha un suo *resource/object identifier* univoco, necessario ad evitare cortocircuiti informatici. I sistemi binari non tollerano ambiguità.

Ma noi, che ci riteniamo i padroni degli strumenti informatici, pur essendo ontologicamente analogici (almeno fino ad oggi), noi abbiamo un'identità univoca all'interno dei sistemi informatici (e in particolare delle reti aperte e dei *social network*)? La risposta è no: noi non abbiamo una nostra univoca identità che ci (rap)presenti nei sistemi informatici.

A mio avviso questa anomalia spiega la maggior parte delle degenerazioni delle reti aperte, che sono sotto gli occhi di tutti. Nessuno dubita che esista un problema di tenuta delle istituzioni democratiche e pluraliste, in un mondo sempre più digitale e (dunque) globalizzato.

Personalmente ritengo che la causa principale delle ben note degenerazioni sia il fatto che i supposti titolari dei sistemi informatici (quali gli iphone, computer, reti domestiche, reti di ufficio, etc.) sono privi di una identità. Gli unici che posseggono una sorta di identità digitale sono i titolari di domini che rilasciano le credenziali di accesso a soggetti terzi: ma tale identità l'hanno solo all'interno del loro dominio; se operano al di fuori di esso divengono, come noi tutti, soggetti passivamente profilati da altri. Diciamo, in via di prima approssimazione, che una identità che è accettata solo "in casa mia" non è quello che noi immaginiamo con la categoria concettuale di "identità".

Un proprietario (di dominio informatico) senza (una vera) identità è, in un certo senso, un ossimoro. Un cavaliere inesistente: nel mondo informatico di oggi si è riproposta la dicotomia fra soggetto ed identità che è esistita per millenni nella società umana. Il diritto (per millenni, fino alla abolizione della schiavitù) ha riconosciuto la soggettività giuridica a determinate persone fisiche; ma non tutte le persone che in teoria erano soggetti di diritto, in pratica possedevano una identità per azionare tali diritti.

Per porre fine a questo stato di cose che si è replicato oggi nel mondo digitale, occorre comprendere cosa sia l'identità, in senso funzionale e giuridico.

Noi giuristi all'università impariamo che il soggetto giuridico (persona fisica o giuridica) è un centro di imputazione di diritti e doveri, munito di una capacità di agire (ossia la capacità di porre in essere condotte giuridicamente rilevanti, ovvero di concludere transazioni giuridiche) piena o limitata. Per noi giuristi l'identità è il fatto fenomenologico (fisico) sotteso al concetto di soggetto giuridico.

I minorenni, gli interdetti e gli inabilitati e le persone giuridiche sono soggetti (identità) con una capacità giuridica limitata. Le persone maggiorenni, capaci di intendere e volere, sono soggetti (identità) con capacità di agire illimitata.

Dato che, fino alla digitalizzazione dei rapporti, l'identità era un fatto esclusivamente fisico, a prima vista sembrerebbe, dunque, che sia impossibile che una persona fisica (o giuridica) sia fenomenologicamente presente all'interno di un sistema informatico, per agire all'interno di esso. Dal punto di vista informatico, siamo soggetti senza identità: nel cyberspazio siamo delle finzioni giuridiche, prive di una fenomenologia sottostante al concetto di "soggetto giuridico". All'interno delle reti telematiche, siamo meno di un fantasma. Infatti, generalmente noi siamo presenti all'interno dei sistemi informatici grazie a un profilo di noi, realizzato dal dominio che "ci ospita" e che ci fornisce le credenziali di accesso al fine di autorizzarci ad agire al suo interno. Nulla a che vedere con la nostra vera identità.

Quel profilo, che non è davvero "me stesso", ma "mi rappresenta" all'interno del dominio, è una entità interamente sotto il controllo del titolare del dominio, che può sospenderla e persino revocarla. Nel mondo fisico nessun o potrebbe revocare o negare la mia identità!

Se si accetta che oggi nel mondo digitale operano degli "avatar[4]" che non hanno con i loro rispettivi titolari una relazione univoca, né sotto il profilo giuridico, né sotto il profilo fenomenologico, forse si comprende la ragione profonda della degenerazione delle relazioni nelle reti aperte e nei cosiddetti social network. Una ragione che sul piano del nesso di causalità si colloca a monte degli algoritmi di ricerca e delle funzioni algoritmiche delle reti aperte e dei (cosiddetti) social network.

Se quello descritto sopra, in poche righe, è il problema, quali sono le possibili soluzioni?

Ritengo che nessuna soluzione possa prescindere da una definizione di identità (digitale) che sia

a) fenomenologicamente vera e
b) funzionalmente idonea a preservare i nostri diritti umani.

In questo contributo, pertanto, proporremo una definizione (giuridica) di identità (digitale), che si manifesti veramente all'interno dei sistemi informatici senza trasformarci tutti in prigionieri virtuali. In questo contributo, inoltre, si evidenzierà come la revisione del Regolamento (UE) 2014/910 (eIDAS), avviata dalla Commissione Europea[5], vorrebbe appunto realizzare tali obbiettivi, anche se la proposta presenta alcuni aspetti problematici.

Il tema di chi siamo per davvero, ossia di quale sia la nostra identità, non si pone oggi per la prima volta: identificare le persone è stato un problema per dieci millenni almeno. La sua ipotetica soluzione risale alla fine del XIX secolo, quando

[4] Per la definizione di avatar, si rinvia a Wikipedia: wikipedia.org

[5] COM (2021) 281 final 2021/0136(COD) consultabile su eur-lex.europa.eu

nei registri delle parrocchie/comunali è stato avviato un censimento di tutte le nascite.

Per comprendere il tema dell'identità e dell'identificazione in una prospettiva millenaria (antropologica), aiuta leggere la vicenda di uno dei primi furti di identità storicamente documentati, frutto di un feroce scherzo ordito da Filippo Brunelleschi (si, lui, l'inventore della prospettiva pittorica e, in sostanza, padre dell'estetica rinascimentale) a Firenze, narrato nella Novella del Grasso legnaiuolo[6].

2. *Dall'identità come status symbol all'identità come onere sociale* - Oggi nel mondo dei social network, quante volte veniamo sottilmente influenzati a vederci come gli altri ci vedono? Probabilmente più spesso di quanto non ce ne rendiamo conto... perché, mentre ai tempi di Manetto il legnaiuolo era ovvio che ciascuno era portatore della propria identità, oggi noi confondiamo facilmente identità e profilo.

Procediamo con ordine. L'identità, prima dei registri parrocchiali (1500 circa) e dello stato civile (1800 circa), non era attribuita alle persone da un documento o da un ufficio, bensì dalla propria linea di sangue, se esistente. Dal tempo dei romani il *Pater Familias* era il soggetto munito di soggettività e capacità di agire che rappresentava gli interessi di tutta la *Familia* e dei famigli ma, nel contempo, era da essa identificato e (per così dire) "certificato"[7].

L'identità, insomma, non era cosa da tutti. L'avevano i patrizi ed altre persone influenti (*aequites*, generali, magistrati) o facoltose. Ma la maggior parte dei cittadini (i plebei), anche se liberi o liberti, alla fine erano definiti dalla gens di appartenenza, non dalla loro famiglia (linea di sangue). Solo coloro che avevano una linea di sangue tracciata e tracciabile, attraverso le primogeniture e le adozioni, ed attraverso una Domus/Villa di residenza della Familia, disponevano oltre che soggettività giuridica anche una vera e propria identità. Chi viveva in un domus/villa altrui o in una insula, se *civis romanus*, aveva soggettività, ma non una sua vera identità, come la intendiamo noi oggi: era definito dal contesto di appartenenza, non dalla propria famiglia/storia. Ciò aveva una immediata ricaduta pratica sull'esercizio dei propri diritti: nel diritto romano (fino al medio evo) gli accordi erano orali, garantiti da testimoni. I contratti scritti erano *notulae*, ossia appunti che riproducevano l'accordo originale, che comunque restava orale. La ragione di ciò, è che pochissimi sapevano leggere e scrivere, i supporti per la scrittura erano costosissimi (papiro, pergamena, ecc.). Pertanto, mentre un patrizio o un *aequites* nel diritto romano trovava all'interno

[6] Per la quale si rinvia a R. GENGHINI, *Identità e profilo: il pericolo di confonderli nella società dell'informazion*e, cit. oppure online wikisource.org.

[7] R. GENGHINI, *Digital New Deal: The Quest for a Natural Law in a Digital Society*, cit., p. 199.

della sua familia/gens un numero sufficiente di persone che fossero disponibili a fungere da procuratori e testimoni, per un plebeo poteva essere molto difficile avere accesso a testimoni che poi effettivamente, ove richiesto, si recassero a testimoniare, si ricordassero i fatti e, soprattutto, non fossero influenzabili.

Le regole romanistiche della primogenitura e dell'adozione/investitura del *Pater Familias* vanno lette anche attraverso la lente della necessità di garantire/certificare l'identità del capofamiglia e del suo patrimonio, al di là di ogni possibile dubbio/conflitto, per garantirgli un effettivo esercizio dei propri diritti e un effettivo accesso alla giustizia.

L'identità nell'antica Roma e nel Medio Evo era, dunque, un privilegio (un vero e proprio *status symbol*) accessibile a coloro che avevano una infrastruttura idonea a identificarli: una famiglia (linea di sangue), un patrimonio e un luogo di origine/residenza. Per chi non aveva questi "asset" identificativi, l'esercizio dei propri diritti dipendeva da fattori esterni, come la gens di appartenenza o la disponibilità di testimoni affidabili.

Ancora nella costituzione rivoluzionaria francese la definizione di cittadino munito del diritto di voto era la seguente: *"Pour être «citoyen actif», il faut avoir au moins 25 ans, résider dans la ville ou le canton depuis au moins une année, être inscrit au rôle de la garde nationale dans la municipalité du domicile, avoir prêté le serment civique et acquitté le paiement d'une contribution directe égale à trois jours de travail. L'Assemblée constituante édifie un régime d'étagement des droits politiques d'après des seuils fiscaux. Elle exclut les pauvres et n'accorde aux moins pauvres que le droit de désigner une minorité d'électeurs fortunés. Ne peuvent être électeurs les «citoyens passifs»: les femmes, les personnes en état d'accusation, les faillis, les insolvables et les domestiques, particulièrement nombreux à l'époque, qui sont exclus du droit de vote comme citoyens non indépendants*[8]*"*. I "citoyens actifs" nel 1790 erano dunque stimati in circa 4 milioni, su una popolazione maschile di 14 milioni. La lettura marxista di queste regole puntava a sottolineare che si restringeva l'accesso al diritto di voto ai poveri, che erano la maggioranza della popolazione. Una diversa lettura, meno ideologica, porta a constatare che si limitasse il diritto di voto ai soli cittadini identificabili, ossia che si erano guadagnati/costruiti una propria identità: avere prestato servizio nella guardia nazionale non era un requisito particolarmente elitario, anche se escludeva molti cittadini che erano malnutriti e malsani. Domestici e famigli, come nell'antica Roma, restano cittadini di serie B, nonostante la rivoluzione... Insomma fino alla istituzione dei registri della popolazione residente, vi erano moltissimi soggetti che non erano non avevano

[8] www.histoire-image.org

una identità (non derivata da altri) e per questo non avevano accesso effettivo ai loro diritti teorici.

Noi che viviamo oggi nella società dei social network, viviamo in prima persona le ricadute terribili che ha sul discorso politico, il fatto che possano intervenirvi a pieno titolo anche soggetti non esistenti, non appartenenti al contesto politico, oppure sedicenti appartenenti (e, dunque, soggetti che per un motivo o per l'altro, "non hanno nulla da perdere").

I registri e gli uffici per la "registrazione e certificazione" della nostra identità sono istituzioni che se, da un lato, esprimevano la volontà dello stato di avere un maggior controllo sulla popolazione, dall'altra facilitavano l'aspirazione della maggioranza della popolazione esclusa dalla cittadinanza attiva, di accedervi. La generalizzazione dello stato civile e dell'anagrafe, rendono obsolete e discriminanti le regole del voto per censo, che quindi saranno abrogate all'inizio del ventesimo secolo[9]. Certamente gli sconvolgimenti della Prima Guerra Mondiale sono stati socialmente e politicamente determinanti nell'estensione del suffragio alle donne e nell'abrogazione del voto per censo. Ma non si può fare a meno di rilevare che la generalizzazione dell'obbligo di registrare le nascite e le morti allo stato civile (fra 1860 e 1880) in Europa, avevano creato (da oltre una generazione) un efficace ed esteso sistema di identificazione (profilazione) di tutti i cittadini e che l'estensione dei diritti politici a tutti, coincide con la messa in opera di una infrastruttura di gestione dell'identità di tutti i cittadini, le cui dimensioni e la cui portata erano assolutamente mai viste prima nella storia dell'umanità.

Se da una parte tale macchina aveva esteso a davvero tutti l'obbligo di leva (come si legge nei Malavoglia) rendendo quasi impossibile sfuggirvi, dall'altra tutti i cittadini beneficiavano di una loro identità di cui lo stato era garante, riducendo enormemente il divario fra chi un'identità propria ce l'aveva e chi, invece, aveva un'identità riflessa, derivata da altri da cui dipendeva (domestici, contadini fittavoli, ecc.).

La storia dimostra che due sono gli elementi indefettibili per la nascita del ceto medio: da una parte il possesso di una identità dimostrabile e dell'altra l'accesso a titoli di proprietà certi[10]. Ciò spiega i programmi di identificazione di massa che sono portati avanti dai paesi in via di sviluppo, come ad esempio l'India e l'Egitto.

È proprio il successo di questa gigantesca macchina di identificazione e profilazione dei cittadini che ha determinato una mutazione del concetto di identità personale. In origine il possesso di una identità era il segno della

---

[9] R. GENGHINI, *Digital New Deal: The Quest for a Natural Law in a Digital Society*, cit., p. 200.

[10] D. ACEMOGLU, S. JOHNSON, J.A. ROBINSON, *Institutions as a Fundamental Cause of Long-Run Growth*. in P. AGHION, S.N. DURLAUF, eds., *Handbook of Economic Growth, 1A ed.*, 2005, Elsevier B.V., pp.385–472

massima realizzazione civile e legale di una persona (essere riuscito a costruirsi una identità così tangibile e reale, da poterla passare alla propria progenie); con la messa in opera di registri dell'anagrafe e dello stato civile omnicomprensivi, in molti stati l'identità si è trasformata in un onere imposto dallo stato al cittadino per riconoscergli (o impedirgli) l'accesso ai suoi diritti[11].

3. *Il mito dell'identificazione come un atto puramente tecnocratico e "neutro" a confronto con la realtà: si tratta di un processo che ha un immediato impatto sui nostri diritti, soprattutto nel contesto digitale* - Chiunque oggi sia dell'idea che l'identificazione sia un mero procedimento tecnico, neutro rispetto alla configurazione ed all'accesso ai nostri diritti, è in errore. Non solo sembra immemore agli orrori dello "*Judenausweis*" ed all'uso politico della carta di identità in Italia sotto Mussolini, ma evidentemente non presta attenzione all'uso strumentale dei processi di identificazione a fini politici non solo nei paesi con sistemi democratici instabili/deboli come l'Etiopia, ma persino negli Stati Uniti d'America!

Fortunatamente le istituzioni europee hanno riconosciuto che l'identità (digitale) è l'architrave necessaria per la tenuta degli ordinamenti giuridici delle nostre democrazie liberali e pluraliste in un mondo digitalizzato ed hanno avviato un processo di legislazione sull'identità digitale, come infrastruttura critica gestita direttamente dagli stati dell'Unione (Capitolo II del Regolamento della Commissione e del Parlamento Europeo (UE) 2014/910 - eIDAS). Una vera identità digitale è il presupposto indefettibile non solo per la piena attuazione del GDPR (Regolamento della Commissione e del Parlamento Europeo (UE) 2016/679), ma anche dei futuri Regolamenti sui servizi informatici (COM 825/2020, del 15 dicembre 2020) e sul mercato informatico (COM 842/2020, del

[11] Non occorre sottolineare quanto questo concetto di identità possa determinare una restrizione dei nostri diritti umani e civili. Non a caso nei sistemi di common-law si è contrari a sistemi estesi di censimento ed identificazione delle persone, per il rischio che questi pongono al libero esercizio dei nostri inviolabili diritti di libertà.
Negli Stati Uniti si sospetta che i programmi di identificazione degli elettori (ben meno stringenti di quelli in essere in Italia o Germania) possano avere la finalità di impedire alle persone socialmente marginali di esercitare il proprio diritto costituzionale al voto. THE ECONOMIST, 21 novembre 2015, *Automatic voter registration. Left Turn*, [online] https://www.economist.com/united-states/2015/11/19/left-turn [Consultato il 22 dicembre 2020]; THE ECONOMIST, 10 ottobre 2020, *Voter suppression. At risk of losing Texas, Republicans scheme to limit Democratic votes* [online] www.economist.com [Consultato il 20 ottobre 2020]. In Etiopia un "eccesso di identificazione" ossia la menzione dell'etnia di appartenenza sulle carte di identità ha reso possibili numerosi ripetuti eventi di razzismo al limite del genocidio: THE ECONOMIST, 6 dicembre 2018, *How to save Ethiopia's democratic revolution* www.economist.com [Consultato il 2 ottobre 2020]; BIEBER, F. GOSHU, W., 15 gennaio 2019, *Don'T Let Ethiopia Become The Next Yugoslavia*. [online] https://foreignpolicy.com [Consultato il 2 ottobre 2020].

15 dicembre 2020). La stessa proposta di revisione del Regolamento (UE) 2014/910 (eIDAS), contenuta nella COM (2021) 281 final 2021/0136(COD)[12] ribadisce che l'identità digitale ed i *wallets* di cui alla proposta di nuovo articolo 6 del regolamento, debbono essere rispettosi della privacy e degli altri diritti fondamentali dei cittadini.

L'opinione dominante, è che la nostra identità "vera", sia quello che sul piano fenomenologico e tecnico si presenta come il nostro profilo amministrativo nel database del registro dello stato civile, in base al quale in Italia vengono emessi la carta di identità ed il passaporto.

In ciò si nasconde un insidioso equivoco, che in una società digitale ha conseguenze molto preoccupanti.

È l'equivoco in cui cade Manetto nella citata novella: egli accetta che la sua identità sia determinata da altri. Ciò a un fiorentino del 1400 può sembrare demenziale e ridicolo, visto che Manetto apparteneva a quel 10% della popolazione che aveva una sua propria identità, che gli derivava dalla linea di sangue della sua famiglia, dalle proprietà (prima, seconda casa, cascina, bottega) e dall'appartenenza alla Mercatura dei legnaiuoli.

Nel momento in cui accettiamo che un record di un database pubblico sia la nostra identità, e che i nostri diritti discendano da esso, abbiamo istantaneamente affievolito la gran parte dei nostri diritti costituzionali digitali, in quanto il loro unico centro di imputazione si trova ed è gestito negli archivi informatici comunali, non presso di noi. Più che titolari di diritti, ne siamo licenziatari.

Finché i nostri diritti potevano essere esercitati solo "offline", recandosi di persona in qualche luogo, è evidente che non aveva alcuna conseguenza l'errore di considerare un profilo amministrativo (per lo più registrato su carta) come la propria vera identità. Comunque, era necessaria la presenza in carne ed ossa, per potere agire ed esercitare i propri diritti, adempiere ai propri obblighi (o esservi costretti).

Ma ora, che tale presenza fisica non è più necessaria, è evidente che se il luogo di residenza della mia "vera identità" è altrove (ad esempio nel dominio del comune, per definizione inaccessibile, oppure in un diverso dominio accessibile, ma regolato da regole e finalità diverse), io opero *in absentia* senza un legale rappresentante legittimato nelle forme di legge: l'unico modo di "essere presenti" in una transazione digitale, è che essa si realizzi (e/o sia provata) grazie alla presenza ed inerenza in essa di un mio identificatore digitale univoco, come potrebbe essere una identità SPID o una smartcard di firma digitale qualificata ai sensi del regolamento eIDAS. Io "esisto" all'interno di un dominio informatico in cui effettuo delle transazioni, solo se il mio "*unique identifier*" (url, IP Address, hash, firma digitale, ecc.) che in quel dominio è il punto di avvio e di riferimento

[12] eur-lex.europa.eu/legal-content

delle transazioni, sia sotto il profilo tecnico/fenomenologico effettivamente connesso a me e sotto il mio controllo esclusivo. La presenza non può essere un artificio concettuale o una finzione giuridica[13]: essa nella dimensione digitale è determinata da procedure come il log-in, la firma, la creazione di un log, ecc.; abbiamo una vera presenza informatica, fenomenologicamente verificabile, solo se i dati della presenza digitale sono riconducibili ad un sistema informatico che è davvero sotto il nostro esclusivo controllo e che ha effettivamente aperto e posto in essere determinate transazioni.

Senza dire che se lo strumento di identificazione on-line che ci viene fornito dallo schema nazionale di identificazione (in Italia lo SPID e la CIE) non è rispettoso dei nostri diritti, ad esempio perché consente il nostro tracciamento, ovvero può essere sospeso/revocato da terzi, è evidente che l'identità (digitale) cesserà del tutto di appartenerci, per divenire una concessione "tecnica" che promana dallo stato e di cui noi cittadini siamo passivi percettori. Alle varie sanzioni amministrative, civili e penali se ne aggiungerà una nuova e devastante: la cancellazione dell'identità, vale a dire la scomparsa del presupposto di qualsiasi diritto di cui un cittadino possa vantare!

Caduto il fascismo in Europa, viviamo da 70 anni in una società aperta e democratica in cui (fino ad oggi) non sono stati messi in discussione (quasi mai) i diritti fondamentali della persona. Tuttavia, l'identità digitale costituisce davvero una "opzione nucleare". Lo stato invece limitarsi ad ignorare i nostri diritti, potrebbe persino ignorare il fatto che esistiamo: o cancellando la nostra identità, o pretendendo che per esercitare certi diritti occorra che siamo identificati online.

Chiunque abbia incontrato, prima della caduta del muro di Berlino, una delegazione di un paese dell'Est europeo, sa che la consegna e la sottrazione dei documenti di identità era una parte essenziale della metodologia di controllo sulle persone. Per potere esercitare i propri diritti era necessaria la presenza in loco non solo della persona, ma anche della prova dell'esistenza del suo profilo amministrativo e della prova che un certo profilo amministrativo davvero si riferisse a quella persona. Non diversamente, oggi, negli Stati Uniti molti ritengono che dalle modalità di identificazione degli elettori dipenda (in larga parte) l'esito delle elezioni politiche[14]. Insomma, nel momento in cui l'unica

[13] Come risulta evidente osservando la condizione sociale e giuridica nella famiglia romana, delle donne, dei figli e degli altri appartenenti alla *familia* diversi dal *Pater familias;* o la condizione del servo della gleba nel Medio Evo. Ogni soggettività priva di una autonoma identità (e/o capacità di agire) si trasforma in una mera finzione giuridica.

[14] THE ECONOMIST, 2015, *Automatic voter registration. Left Turn*, www.economist.com/united-states; THE ECONOMIST, 2020, *Voter suppression. At risk of losing Texas, Republicans scheme to limit Democratic votes* www.economist.com.

identità "vera" ed ammissibile sia quella su cui lo stato ha il monopolio, tutti i diritti che vengono riconosciuti alla mia persona divengono puramente teorici, perché subordinati alla esistenza di quella unica "vera" identità.

Ecco perché, non solo nel mondo di internet, ma in qualsiasi ordinamento giuridico, la mia identità non può essere ridotta alla esistenza di un mio profilo amministrativo, ma si deve riconoscere che esiste una sola vera identità ed è appunto quella che si incorpora e sostanzia realmente nella mia persona. Ogni finzione di identità è una minaccia letale alla libertà ed alla certezza del diritto.

Non erano liberi gli schiavi che per il diritto romano erano oggetti parlanti (*instrumenta vocalia*) privi non solo di soggettività, ma anche di identità; non erano liberi (nella odierna accezione del termine) donne, famigli e liberti, che a Roma necessitavano del supporto di una *Familia* per potere esercitare i loro diritti; non erano liberi i servi della gleba, che erano identificati attraverso la terra cui appartenevano e il luogo in cui su di essa vivevano, con divieto di abbandonarla, a pena della loro stessa vita; non siamo liberi oggi noi nelle reti aperte e nei network sociali, nei quali l'identità ci viene attribuita ed è gestita da altri che gestiscono i domini in cui ci muoviamo, senza alcuna nostra possibilità di influire su di essa... . Come se non bastasse, noi non possiamo fuggire da Internet; e neppure potremmo fuggire dallo stato che dovesse smarrire o cancellare la nostra identità digitale. Significa che nel mondo digitale cade il fondamento teorico degli stati liberali, come teorizzato da Hobbes[15], Locke[16] e Rousseau, quale adesione ad un "contratto sociale"[17] (o rifiuto di esso): chi è privo/privato della propria identità non può aderire, né rifiutare il contratto sociale e da persona viene giuridicamente degradato a fatto o cosa (come, appunto, gli schiavi).

Insomma, a ben vedere, l'identità nei secoli è stata una faticosa affermazione di chi siamo, che riusciva ad una minoranza di capaci/fortunati/privilegiati. Nel momento in cui le istituzioni hanno reso possibile a tutti l'accesso ad una identità, il concetto di identità e di profilo amministrativo si sono sovrapposti e confusi, per il fatto che fosse ontologicamente impossibile che qualcuno fosse presente e identificabile/identificato, senza essere in loco.

Tuttavia, le esperienze dei regimi totalitari della fine del diciannovesimo e della prima metà del ventesimo secolo ci hanno mostrato come imporre una sola unica identità (quella statale) come presupposto per avere accesso ai propri diritti, è suscettibile di divenire una grave forma di repressione, strumentale persino al genocidio[18].

---

[15] T. Hobbes, *Leviathan (1651)*, 2017, Penguin Classics.

[16] J. LOCKE, *The First & Second Treatises of Government (1689)*, 1998, Cambridge University Press.

[17] J. J. ROUSSEAU, *Du Contrat social* (1762), 2011, Paris Flammarion.

[18] R. GENGHINI, *Digital New Deal: The Quest of a Natural Law in a Digital Society*, cit., p. 206.

Posto che nella dimensione digitale tutto è frutto di design ed implementazione, deve essere chiaro che se il design e l'implementazione dell'identità digitale ci vede tutti deformi, con un occhio solo e incatenati, tale sarà la nostra identità digitale; tali saranno i soggetti che popolano il cyberspazio del futuro.

Se, invece, il design e l'implementazione dell'identità digitale non solo difendesse i nostri attuali diritti civili, ma, addirittura, li ampliasse, i nostri ordinamenti liberali, pluralistici e democratici ne uscirebbero rafforzati[19]. Due esempi:

1) Controllo di polizia stradale: "patente e libretto per favore". Orbene con una buona implementazione dell'identità digitale l'ufficiale di polizia stradale potrebbe essere certo che il conducente ha i documenti in regola, senza dovere conoscere l'identità del soggetto controllato. Persino nel caso di una infrazione al codice della strada (che non viene sanzionata con punti, la revoca della patente o l'arresto) potrebbe applicare le sanzioni senza sapere chi sia il soggetto sanzionato. Laddove si tratti di infrazioni gravi l'ufficiale di polizia stradale le contesta e, come conseguenza della contestazione, il gestore dello schema nazionale di identificazione gli mette a disposizione gli attributi di identificazione del conducente. Oggi ciò è impossibile e tale impossibilità riduce la reale portata dei nostri diritti civili, per cui un normale controllo di polizia stradale si trasforma in una invasione della nostra sfera personale.

2) *Wistleblowing*: oggi la segnalazione di un abuso da parte di un organo dello stato o di una organizzazione criminale o è davvero anonima (per cui potenzialmente poco credibile) o rivela l'identità del segnalante (che resta esposto a ritorsioni). Con una buona implementazione dell'identità digitale vi potrebbero essere due tipi di segnalazione anonima: una del tutto anonima, come le attuali; ed una in cui il segnalante si assume la piena responsabilità della segnalazione senza perdere l'anonimato. In questo secondo caso l'autorità cui perviene la segnalazione è certa che, in caso di calunnia o altro reato, potrà identificare e perseguire il segnalante, senza che sia necessario che il segnalante resti in balia di ulteriori ritorsioni illegittime da parte dei soggetti segnalati.

Non è importante discutere adesso se tali nuove possibilità, che deriverebbero da una "buona" implementazione dell'identità digitale, siano un "miglioramento" o un "peggioramento" delle attuali regole: ciò che conta è che si

[19] Come ha rilevato la Presidente dell'Unione Europea, URSULA VON DER LEYEN, nel suo *State of the Union Address at the European Parliament Plenary 16th September 2020* ec.europa.eu

tratta di esempi che fanno capire che l'identità digitale (a seconda di come implementata) apre scenari e dimensioni di tutela/violazione dei nostri diritti che sono semplicemente inconcepibili in un mondo analogico: la semplice esistenza di un Wallet di identità digitale, in altre parole, ha come effetto inevitabile una trasformazione del modo di esercitare i propri diritti ed adempire ai propri doveri e una metamorfosi della forma dei documenti giuridici che saranno sempre più registrazioni di operazioni telematiche (anche se in presenza fisica) e sempre meno documenti statici.

Il "minimo sindacale" che l'identità digitale dovrà garantire nella dimensione digitale, tuttavia, è che noi si possa navigare in rete, né più e né meno di come facciamo oggi quando passeggiamo per le strade della nostra città (in assenza di videocamere di sorveglianza): incontriamo altre persone, visitiamo negozi e uffici, senza lasciare una traccia indelebile di noi, eppure coloro che interagiscono con noi sanno che siamo esseri umani (non androidi o troll o altri oggetti inumani) e ricevono da noi solo le informazioni che noi decidiamo di mettere loro a disposizione.

A tal fine sarebbe auspicabile che l'identità digitale fosse garantita e protetta da un "*freedom device*"[20], capace di replicare ed espandere sul piano informatico ciò che nel mondo fisico sono le libertà fondamentali che le nostre carte costituzionali riconoscono e tutelano.

4. *I Wallet*[21] *come strumento di protezione dell'identità personale e di volontaria presentazione dei propri attributi* - Prima di definire cosa possa essere un Wallet in cui proteggere/gestire personalmente la propria identità digitale, occorre proporre una definizione di cosa siano le identità digitali.

Già nel 1996 da C. Ellison ha lavorato ad una definizione di identità che non dipendesse da una fonte esterna unica[22]. Poco meno di un decennio dopo, studi

[20] R. GENGHINI, *Digital New Deal: The Quest for a Natural Law in a Digital Society*, cit., p. 257.
[21] L'articolo 3 (42) della proposta di modifica del regolamento eIDAS definisce il Wallet come "*portafoglio europeo di identità digitale",* ossia *un prodotto e servizio che consente all'utente di conservare dati di identità, credenziali e attributi collegati alla sua identità, fornirli su richiesta alle parti facenti affidamento sulla certificazione e utilizzarli per l'autenticazione, online e offline, per un servizio, conformemente all'articolo 6 bis, nonché per creare firme elettroniche qualificate e sigilli elettronici qualificati"*;
[22] C. ELLISON, *Establishing Identity without Certification Authorities*", 6th USENIX Security Symposium, 1996, www.usenix.org

europei[23] e statunitensi[24] sono giunti a più precise conclusioni, sotto il profilo della privacy e dei diritti fondamentali della persona: l'identità digitale si distingue dal profilo digitale perché è liberamente scelta dal soggetto. Il profilo digitale, invece, è costruito da un soggetto terzo che, di solito, è il gestore di un dominio o di una piattaforma (nel linguaggio del legislatore europeo, si tratta di "*large platforms*" e di "*gatekeepers*")[25]. Ne consegue che anche la nostra "identità statale/amministrativa" è un profilo di noi, gestito dallo stato, non la nostra identità personale[26]. Pertanto, in funzione della nostra libertà di espressione, possiamo adottare più identità (digitali): ad esempio, quella di padre, frequent flyer, socio della bocciofila, abbonato al Corriere della Sera, eccetera.

Sul filone di queste ricerche si colloca il concetto di "*self sovereign identity*", affermatosi sul piano tecnico, anche grazie al lavoro del W3 Consortium sull'architettura dei *Decentralized Identifiers (DIDs)*[27].

Insomma, nel mondo fisico il nostro corpo è, in base ai principi costituzionali, esclusivamente sotto la nostra titolarità (*habeas corpus*); l'equivalente nel mondo digitale è che noi si debba essere liberi di gestire le nostre identità digitali, fermo restando che nel momento in cui interagiamo con la pubblica amministrazione può essere necessario usare il proprio profilo attribuitoci dallo stato, mediante i documenti di identità o gli schemi nazionali di identificazione (in Italia lo SPID e la CIE).

Questa corretta definizione di identità (digitale) mostra l'enorme importanza che ha nel contesto digitale lo strumento tecnologico che deve mettere noi in condizione di proteggere e gestire online ed offline il nostro profilo amministrativo attribuitoci dallo stato e le altre identità da noi scelte ed i relativi attributi.

---

[23] M. HANSEN, H. KRASEMANN, M. ROST, R. GENGHINI: *Datenschutzaspekte von Identitätsmanagementsystemen*; in: *DuD*, 2003, 551; M. HANSEN, R. GENGHINI *Identity Management Systems (IMS): Identification and Comparison Study Independent Centre for Privacy Protection (ICPP) /* Unabhängiges Landeszentrum für Datenschutz (ULD) Schleswig-Holstein and Studio Notarile Genghini (SNG), 2003-09-07, Contract N°19960-2002-10 F1ED SEV DE www.genghinieassociati.it, www.semanticscholar.org; REPKINE, ALEXANDRE HWANG, JUNSEOG, *A Network-Economic Policy Study of Identity Management Systems and Implications for Security and Privacy Policy* (2004), mpra.ub.uni-muenchen.de; M. HANSEN, P. BERLICH, J. CAMENISCH, S. CLAUß, *Privacy-Enhancing Identity Management*, March 2004 in *Information Security Technical Report* 9(1):35-44, www.researchgate.net.

[24] S. T. KENT *Who Goes There?: Authentication Through the Lens of Privacy*, 2003, Proceedings of the US National Academy of Science.

[25] Il Digital Markets Act, EU Commission COM 842/2020, del 15 dicembre 2020, ec.europa.eu e il Digital Services Act, EU Commission COM 825/2020, del 15 dicembre 2020, eur-lex.europa.eu.

[26] R. GENGHINI, *Digital New Deal: The Quest for a Natural Law in a Digital Society*, cit., p. 193 ss.

[27] www.w3.org.

La proposta (COM 281/2021) di modifica del Regolamento (UE) 2014/910 (eIDAS), propone il concetto di "*European Digital Identity Wallet*" agli articoli 3(42) e 6a e ss., come strumento che ha la finalità di consentirci di avere il controllo esclusivo sui nostri attributi identificativi in tutte le relazioni online e offline. Purtroppo, come anche rilevato da numerosi esperti, anche nelle audizioni del Parlamento Europeo, il concetto di Wallet è assai generico, potendosi riferire ad almeno tre famiglie di soluzioni tecnologiche assai diverse fra loro, che fanno principalmente uso dei profili amministrativi attribuiti dallo stato al cittadino:

1) un primo gruppo fa uso degli smartphone e della firma digitale, senza però che vi sia installato su di essi una App di gestione dell'identità digitale;

2) un secondo gruppo fa uso di canali sicuri di comunicazione fra un terminale dell'utente (computer, cellulare, ecc.) e le infrastrutture centralizzate presso le quali sono conservate e gestite le identità digitali;

3) un terzo gruppo utilizza delle app gestionali dell'identità digitale residenti sul terminale del cittadino, senza che vi sia un sistema centralizzato di gestione dell'identità digitale[28].

Lo studio di fattibilità[29] e lo studio di verifica di impatto[30] della riforma del Regolamento eIDAS, entrambi rilevano che uno strumento di gestione dell'identità digitale debba avere una serie di funzioni essenziali, ripetutamente menzionate nella bozza di revisione del Regolamento:

1) Proporre una interfaccia comune per i servizi di identificazione ed autenticazione (articolo 6a (4a) della proposta di revisione del Regolamento);
2) Essere sotto l'esclusivo controllo del titolare (consideranda (2), (7) e articolo 6a (7) della proposta di revisione);
3) Consentire al titolare *di richiedere e ottenere, conservare, selezionare, combinare e condividere in modo sicuro, trasparente per l'utente e tracciabile da quest'ultimo, i dati giuridici di identificazione personale e gli attestati elettronici di attributi necessari per l'autenticazione online e offline al fine di utilizzare servizi pubblici e privati online* (articolo 6a (3a) della proposta di revisione);
4) Non consentire il tracciamento delle attività del titolare (articolo 6a (4b) della proposta di revisione).

---

[28] Per una dettagliata descrizione dei sistemi esistenti nei diversi stati membri dell'Unione si rinvia a: 1) *Evaluation study of the Regulation no.910/2014 (eIDAS Regulation) SMART 2019/0046 Final Report*, eur-lex.europa.eu; 2) *Study to support the impact assessment for the revision of the eIDAS regulation Final Report Contract number: SMART 2019/0024 VIGIE number: 2020/666* op.europa.eu/

[29] V. nota precedente.

[30] V. nota 28.

Tutto ciò dimostra che sono infondati i timori di alcuni che paventano che l'identità digitale che l'Unione Europea intende introdurre, sia sintomatica della volontà (politica?) di conseguire un controllo orwelliano sui cittadini europei. Ciononostante, è vero che la proposta di regolamento non fornisce una serie di garanzie legislative che sarebbero necessarie per assicurare che, neppure per sbaglio, possa accadere che il Wallet si trasformi in uno strumento che, invece di proteggere ed espandere i nostri diritti, divenga esclusivamente la *longa manus* dello stato, quando ci vuole tracciare e/o rintracciare.

Tali garanzie sono contenute nel Capitolo III del vigente regolamento eIDAS discusso ed approvato dal Consiglio e dal Parlamento europeo il 23 luglio 2014 e hanno garantito l'uniforme applicazione in Europa del Regolamento, fornendo solide basi di riferimento agli enti di standardizzazione tecnica chiamati a fornire le relative norme tecniche di attuazione[31].

Nel prossimo paragrafo si proporrà l'insieme delle funzionalità che uno strumento di gestione dell'identità digitale deve possedere, per potere essere un "*freedom device*". Tali funzionalità andrebbero espressamente disciplinate nella revisione del Regolamento eIDAS, per consentire la redazione di regole tecniche implementative del Regolamento, che siano sicure e tecnologicamente neutrali, come esplicitamente richiesto dal Regolamento stesso!

5. *Opportunità e rischi del Wallet: come disciplinarlo e implementarlo correttamente* - Uno strumento di identificazione/autenticazione elettronica, per potere assolvere alla sua funzione senza divenire un pericolo per la privacy ed i diritti civili, deve (come la moglie di Cesare) non solo essere onesto, ma anche sembrarlo[32]. Fuor di metafora, significa che le sue proprietà tecniche, di cui si dirà appresso in questo paragrafo, non possono essere semplicemente affermate, ma debbono essere puntualmente verificate (come anche la proposta di revisione del Regolamento eIDAS prevede all'articolo 6c). L'Europa si è dotata di un sistema di vigilanza e di verifica di conformità per i servizi elettronici di fiducia, ai sensi degli articoli 19 e 24 del Regolamento eIDAS, che trova nello standard ETSI EN 319 401[33] le sue norme tecniche implementative. L'accreditamento dei CAB *Conformity Assessment Bodies* avviene in base alla EN 319 403 V2.2.2 (2015-

[31] Si tratta di ETSI e Cen-Cenlec. Per una lista completa degli standard attuativi del regolamento aggiornata al 2018, v. il rapporto di ENISA *Assessment of Standards related to eIDAS* www.enisa.europa.eu. Per l'elenco completo degli standard ETSI aggiornati ad oggi v. portal.etsi.org.

[32] R. GENGHINI, *Digital New Deal: The Quest for a Natural Law in a Digital Society*, cit., p. 207 e 237, ss. In cui si spiega l'esigenza di una "*enhanced net neutrality*" vale a dire di modelli di cybersecurity che siano trasparenti, imparziali e verificabili.

[33] ETSI ESI EN 319 401 V2.3.1 (2021-05) *Electronic Signatures and Infrastructures (ESI) General Policy Requirements for Trust Service Providers:* consultabile al seguente URL: www.etsi.org.

08) che specifica ed adatta lo standard ISO/IEC 17065 alle esigenze di sicurezza informatica, organizzativa e fisica dei prestatori di servizi di fiducia qualificati[34]: tutti gli stati membri dell'Unione, in questo momento, svolgono la propria vigilanza seguendo i due standard tecnici di ETSI, senza che siano emersi problemi di sicurezza o di inadeguatezza delle relative norme tecniche[35]. L'attuale schema di vigilanza e di verifica di conformità eIDAS è uniforme in Europa ed è comunque inquadrato nell'ambito delle attività di verifica di conformità disciplinate dal Regolamento (UE) 2019/881 (Cybersecurity Act)[36], che richiama espressamene il Regolamento eIDAS.

Affinché uno strumento di gestione dell'identità digitale possa funzionare, senza divenire uno strumento diabolico di tracciamento e controllo della nostra vita, occorre innanzitutto distinguere l'identificazione dell'autenticazione, cosa che l'attuale proposta non fa con sufficiente chiarezza.

L'identificazione è il processo in cui:

---

[34] EN 319 403 V2.2.2 (2015-08) *Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers* www.etsi.org.

[35] Il caso di Diginotar en.wikipedia.org è antecedente al Regolamento eIDAS. Fu proprio il caso Diginotar a determinare la Commissione Europea a emanare un regolamento, in luogo di una direttiva, al fine di garantire che la vigilanza e la verifica di conformità dei prestatori di servizi di fiducia fosse soggetta a regole europee e non nazionali. Da questo punto di vista il rinvio alla proposta di direttiva NIS2 rappresenta un passo indietro, non un passo avanti.

[36] Appare dunque incomprensibile perché la proposta di revisione del Regolamento eIDAS voglia trattare i prestatori di servizi di fiducia alla stregua di infrastrutture critiche, richiamando la c.d. Direttiva NIS2: *Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 COM/2020/823 final* consultabile al seguente URL: eur-lex.europa.eu.

Per un verso è eccessivo, in quanto un sistema di marche temporali, di recapito elettronico certificato o di verifica delle firme certo non ha alcuno dei requisiti di una infrastruttura critica, né tali servizi presentano i rischi di impatto di una diga o di una centrale elettrica o nucleare: le metodologie intrusive ed altamente formalizzate degli audit delle infrastrutture critiche rischia di mettere fuori mercato i prestatori di servizi di fiducia che non abbiano le dimensioni di una telecom, di una utility o di un gestore di servizio postale. Il che sarebbe del tutto contrario alla finalità del regolamento eIDAS che, invece, intende aprire il mercato dei servizi di fiducia anche a società informatiche piccole e medie. Cosa che ha saputo fare con enorme successo: 20 anni fa esisteva un quasi monopolio delle firme digitali, gestito da due società RSA e Verisign; oggi i numerosi certificatori europei e gli standard europei sono leader a livello mondiale.

Per un altro verso è insufficiente, in quanto i requisiti delle infrastrutture critiche oggi esistenti non toccano gli aspetti specifici della sicurezza crittografica, organizzativa, fisica e informatica che deve avere un prestatore di servizi di fiducia qualificato che emette certificati qualificati di firma, di identità/attributi.

E per un ultimo verso del tutto inadeguato, in quanto i la proposta di Direttiva NIS2 prevede tempi di almeno 3 anni per la creazione dei nuovi schemi di verifica di conformità che, quindi, oltre ad essere per un verso eccessivi, per un altro insufficienti, alla fine sarebbero anche tardivi.

Non si comprende perché la Commissione Europea voglia rischiare un blocco totale dei servizi di fiducia, che oggi sono un modello che viene imitato a livello internazionale.

a) si definiscono una serie di attributi che, secondo una determinata policy, sono identificativi di una persona;

b) si collegano detti attributi ad un token tecnologico, che costituisce la rappresentazione informatica della detta identità.

Il processo di identificazione può essere svolto in due modalità complementari ma fondamentalmente diverse:

A) l'identificazione è effettuata dal soggetto identificato: in tal caso si ha una vera e propria identità (*claimed identity*) che, se sotto il controllo esclusivo del titolare, diviene anche una *self sovereign identity*;

B) oppure, in alternativa, l'identificazione è effettuata da un soggetto terzo:

I. da una "*fonte autentica*" (articolo 3 (46) della proposta di revisione): in tal caso si tratta del profilo amministrativo riconosciuto dallo stato, che nella proposta di Regolamento però non è definita funzionalmente, anche se per essa di usa il termine "*identità digitale*" o "*identità elettronica*".

II. da un soggetto terzo di fiducia (*Trusted Third Party "TTP"*) che, pur non avendo fede pubblica e potestà certificatorie, dispone delle competenze tecniche e dell'infrastruttura (organizzativa e tecnica) necessaria al fine di attribuire ad un soggetto una identità digitale[37].

In generale la proposta di revisione del Regolamento eIDAS configura l'European Digital Identity Wallet come uno strumento tecnologico che deve abilitare i cittadini dell'Unione a mantenere sotto il proprio esclusivo controllo la propria identità digitale, per cui come uno strumento per la *self sovereign identity*. La proposta di modifica del Regolamento, tuttavia, menziona la *self sovereign identity* nella relazione di presentazione e in un considerando[38], ma omette di disciplinarla compiutamente, sia come principio generale, sia nel dettaglio: una mancanza grave se si considera l'enorme rilevanza sistematica della (vera) identità digitale, ossia dell'identità che noi scegliamo liberamente di adottare e che si trova tecnologicamente sotto il nostro esclusivo controllo[39]. La proposta di regolamento non chiarisce il processo funzionale di attribuzione di una identità ad un soggetto, né se tale attribuzione è una auto-attribuzione (*claimed identity)*, né se è fatta da terzi *(attributed identity*), come nel caso di una "*fonte autentica*" o come nel caso di un prestatore di servizi di fiducia qualificato, ai sensi dell'articolo 45-sexies della proposta di revisione del Regolamento.

---

[37] Modalità che non sarebbe consentita nel caso di presentazione dell'identità digitale ad un servizio pubblico: v. articolo 45b della proposta di revisione del Regolamento eIDAS.

[38] Considerando (34)

[39] Anche nei citati studi di fattibilità e di impatto, vi sono numerosi riferimenti alla *self sovereign identity*

La mancanza di tali definizioni essenziali rende di conseguenza impossibile distinguere nel Regolamento l'identificazione dall'autenticazione.

La vigente definizione tecnica di autenticazione del Regolameneto eIDAS è errata/incompleta/generica, dato che essa era stata formulata in primis per descrivere la modalità tecnica di verifica tecnica di una firma elettronica avanzata/qualificata applicata ad un oggetto informatico (v. articolo 3 (5)). Essa andrebbe sostituita con una definizione che sia consistente con quelle tecniche vigenti ed universalmente accettate: ad esempio, sulla scorta della definizione ISO, si potrebbe dire che "*autenticazione é il processo elettronico nel quale una persona fisica o giuridica presentano uno o più attributi per la loro validazione nei confronti di una serie di requisiti tecnici e/o legali al fine di ottenere l'acceso (online o offiline) ad un determinato dominio o sistema informatico al fine di eseguire determinate interazioni informatiche*". [40]

Si commenta da sola la circostanza che, pur essendo previsti nella proposta di revisione del Regolamento (diffusamente e ripetutamente!) servizi di autenticazione, essi non vengono definiti e non assurgono al rango di servizi elettronici di fiducia: ciò è davvero problematico, perché l'unico modo di rendere compatibile il Regolamento eIDAS con i dettami del GDPR, in particolare dell'articolo 32 (*privacy by design* e *data minimisation*), è di implementare servizi di autenticazione sulla base della tecnica cosiddetta "*zero knowledge*"[41] che è anche ripetutamente menzionata nei citati studi di fattibilità e di impatto della revisione del Regolamento eIDAS.

Se esistessero delle adeguate definizioni tecniche di identificazione ed autenticazione, sarebbe chiaro che il Wallet, nella sua configurazione più estesa, potrebbe essere oltre che strumento di identificazione, anche strumento di autenticazione. Invece nella proposta della Commissione Europea a volte sembra che debba necessariamente essere entrambe le cose.

La componente di identificazione sarebbe soggetta alle regole del Capitolo II del Regolamento, per cui la sua sicurezza sarebbe responsabilità diretta degli stati membri dell'Unione.

La componente di autenticazione sarebbe soggetta (almeno in parte) alle regole del Capitolo III del Regolamento, per cui sarebbe un servizio elettronico di fiducia, semplice o qualificato, la cui certificazione di sicurezza avviene secondo lo schema europeo di accreditamento dei prestatori di servizi elettronici di fiducia qualificati.

Se la terminologia della proposta di riforma del Regolamento eIDAS fosse consistente e chiara, sarebbe evidente che non è affatto pacifico che sia opportuno che un Wallet (vigilato ai sensi del Capitolo II del Regolamento eIDAS) abbia

[40] V. ISO/IEC 29115 che rinvia a ISO/IEC 18014-2.

[41] Per tutti si rinvia a abc4trust.eu.

anche funzioni di autenticazione (vigilate ai sensi del Capitolo III del Regolamento). Infatti le proposte di compromesso della Presidenza francese del Consiglio auspicano che il Wallet non abbia anche funzioni di autenticazione.

Inoltre l'assenza di una disciplina dei servizi elettronici di autenticazione (come servizi elettronici di fiducia qualificati) nella revisione del Regolamento eIDAS impedisce la soluzione di una serie di problemi che la proposta della Commissione europea ha correttamente evidenziato, senza proporre però delle soluzioni funzionali/funzionanti:

1) innanzitutto, come si vedrà appresso, il tema della privacy e della tutela dei diritti inviolabili dei cittadini. Le previsioni degli articoli 6c, 12 (dal quale è stato curiosamente eliminato il richiamo al GDPR) e 17 non sono davvero sufficienti, soprattutto visto che l'articolo 5 si limita, in modo assolutamente inadeguato, ad affermare che l'uso degli pseudonimi è ammesso. In realtà il GDPR li impone, in particolare all'articolo 32 che afferma i principi di minimizzazione dei dati e di *privacy by design*;
2) in secondo luogo, il problema delle *relying parties* (parti facenti affidamento sui Wallets e i relativi schemi di identificazione/autenticazione), che l'articolo 6b correttamente individua come componente essenziale del modello di sicurezza dell'identificazione (e autenticazione) informatica. Orbene, queste non sono prestatori di servizi di fiducia eppure, possono accedere (o attivare) il Wallet, con evidenti insormontabili problemi di sicurezza e privacy. La generica disposizione che questi soggetti debbano rispettare il diritto dell'Unione non risolve affatto il problema. Perché il modello di sicurezza sia funzionale, occorre che questi soggetti siano anch'essi sottoposti a vigilanza, ma ciò è impossibile, perché in caso di successo degli schemi nazionali di identificazione, i principali utilizzatori dei Wallet sarebbero i *gatekeepers* e le *large platforms*;
3) infine, i servizi di autenticazione qualificata potrebbero costituire una prima soluzione che consentirebbe ai Wallet di essere utilizzati nelle transazioni elettroniche, persino qualora i produttori di *smartphones* si rifiutassero di consentire ai Wallet europei di accedere alla componente sicura dei terminali da loro prodotti. Si pensi che persino i certificati per l'autenticazione dei siti web (QWACs) sono stati stata rigettati dalla comunità dei browser (che oggi ha il monopolio dell'identificazione e autenticazione dei siti web) con il pretesto che essi pongano un rischio di sicurezza, benché si tratti di file ascii senza codice attivo. Non è difficile figurarsi come reagiranno i produttori di *smartphones* (ciascuno dei quali è un monopolista all'interno del suo sistema informatico) ad un Wallet:

esso è un software crittograficamente protetto e costituisce una pericolosa black-box per il sistema informatico che lo ospita.

La mancanza di una adeguata definizione di autenticazione ha una ulteriore conseguenza, che manchi chiarezza sulla natura degli attributi. Infatti, gli attributi possono essere:

1) auto-dichiarati: ciò deve essere possibile proprio come espressione della libertà di pensiero ed espressione;
2) attestati da un generico service provider: ciò deve essere possibile per la medesima ragione di cui sopra. Sarebbe grave che attestati di frequenza, dichiarazioni di enti e organizzazioni sociali possano essere emesse solo su carta e non possano avere forma digitale! In tal caso si tratterebbe di meri attributi;
3) attestati da un prestatore di servizi elettronici di fiducia qualificato (attributi qualificati)
4) certificati da una fonte autentica.

Immaginando che il Regolamento eIDAS disponga di adeguate definizioni di autenticazione e identificazione (nelle sue tre varianti: auto-identificazione, identificazione da fonte autentica e identificazione da prestatore di servizi di fiducia), quali sarebbero le funzioni tecniche essenziali affinché un cittadino possa avere ragionevole fiducia che il suo Wallet non costituisca una intollerabile diminuzione dei suoi diritti fondamentali?

Ecco le funzioni tecniche che si ritiene necessario che la legge fissi in modo inderogabile, anche al fine di consentire la realizzazione di standard tecnici di implementazione che siano, allo stesso contempo, sicuri e tecnologicamente trasparenti e neutrali. Si noti che, per ragioni tecniche (ed al fine di garantire la necessaria neutralità tecnologica), come nel caso della firma digitale, occorre che gli strumenti di autenticazione possano essere sia avanzati, sia qualificati. La differenza consiste nel fatto che uno strumento di autenticazione avanzato è auto-dichiarato tale. Lo strumento di autenticazione qualificato, invece, è certificato come qualificato da uno schema europeo (si auspica, non da 27 schemi nazionali, come attualmente previsto dalla proposta di revisione del Regolamento eIDAS) di certificazione della sicurezza informatica.

Lo strumento di autenticazione elettronica avanzata deve assicurare mediante procedure e mezzi tecnologici adeguati come minimo che:

a) è ragionevolmente assicurata la riservatezza dei dati per l'autenticazione elettronica utilizzati;
b) i dati per la gestione di una autenticazione elettronica possono comparire in pratica una sola volta;
c) i dati gestione di una autenticazione elettronica non possono, con un grado ragionevole di sicurezza, essere derivati e l'autenticazione

elettronica è attendibilmente protetta da contraffazioni compiute con l'impiego di tecnologie attualmente disponibili;

d) i dati per l'autenticazione elettronica utilizzati possono essere attendibilmente protetti dal firmatario legittimo contro l'uso da parte di terzi.
e) i dati contenuti nello strumento di identificazione/autenticazione elettronica non possono essere creati, modificati o cancellati senza il consenso esplicito del titolare;
f) lo strumento di identificazione/autenticazione elettronica possa essere solo installato e disinstallato dal suo legittimo titolare;
g) lo strumento di identificazione/autenticazione elettronica accetti tutti i formati di attributi qualificati e avanzati riconosciuti in standard europei o internazionali
h) lo strumento di identificazione/autenticazione elettronica fornisca solo al suo legittimo titolare il tracciamento di tutte le operazioni di identificazione o autenticazione realizzate a suo mezzo
i) lo strumento di identificazione/autenticazione elettronica presenti, ove richiesto, i dati di identificazione personale così come determinati dallo stato membro competente.

Per chi è familiare con la attuale struttura del Regolamento eIDAS, si tratta di una replica, dell'Allegato II (relativo agli strumenti di generazione della firma elettronica qualificata), con i necessari adattamenti, alle esigenze di uno strumento di identificazione e autenticazione.

La mancanza della determinazione di questi requisiti funzionali e di sicurezza nella attuale proposta di revisione del Regolamento ha due conseguenze che andrebbero assolutamente evitate:

1) Non esclude, come visto, il rischio che, nonostante le migliori intenzioni della Commissione Europea, gli strumenti di autenticazione elettronica si trasformino in macchine liberticide, come è accaduto per le carte di identità in Eritrea o per i cellulari in Cina
2) Rende impossibile la standardizzazione tecnica degli strumenti di autenticazione.

Il Consiglio e il Parlamento europei stanno affrontando il tema con estrema attenzione e hanno a tal fine esteso di almeno due mesi il calendario dei lavori approvazione della proposta di revisione del Regolamento eIDAS, che si concluderà, salvo ulteriori rinvii, sotto la presidenza Ceca o quella Svedese.

6. *Conclusioni: l'identità (digitale) non può essere una mera finzione giuridica ed occorre che ce ne riappropriamo con la consapevolezza della sua enorme importanza* - L'identità per assolvere alla sua funzione non può essere

semplicemente un profilo, né una finzione giuridica. Essa deve esistere fenomenologicamente per davvero e deve pertanto essere connessa alla nostra persona in modo univoco e sicuro, grazie alle funzionalità brevemente schematizzate nel paragrafo precedente.

L'attuale situazione (in assenza di uno strumento di identificazione/autenticazione elettronica sicuro, trasparente e tecnologicamente neutrale), in cui le nostre cosiddette identità digitali sono a noi imposte e gestite dai proprietari di *large platforms* e *gatekeepers* ha una serie di importanti implicazioni:

a) nel mondo delle transazioni digitali attualmente si opera sulla base di una serie di finzioni e di presunzioni che ci espongono a tutti i rischi e le conseguenze giuridiche che derivano dall'avere effettivamente partecipato a tali transazioni, anche se molte delle tutele fondamentali alle quali potremmo e dovremmo aspirare (riservatezza, divieto di profilazione), ci sono negate in quanto siamo "*sans papier*", rappresentati da una identità "non vera" puramente presuntiva ed effimera (valida solo all'interno del dominio della transazione, ossia generata ed autocertificata dalla nostra controparte transazionale). Occorre rivedere tali finzioni e presunzioni, alla luce della giurisprudenza romana sui negozi fra *Pater Familias* e famigli, ed alla luce dei diritti fondamentali della persona, che non possono affievolire a causa delle prassi che sono invalse nel commercio elettronico. È falso dire che abbiamo spontaneamente rinunciato ai nostri diritti: ci siamo stati costretti, a pena di rimanere esclusi da gran parte del commercio giuridico e delle interazioni sociali. Il ricatto funziona come tutti sappiamo: "*se vuoi fare parte di Instagram, Facebook, Amazon, Apple, ecc. devi consentirci di raccogliere dati su quello che fai, in modo che noi possiamo generare un Tuo profilo per poterci fidare che sei Tu. Ma se non sei d'accordo, resti fuori*". A questo punto è diventato necessario che rivendichiamo il diritto ad essere identificati dalla nostra vera identità (e non da un surrogato gestito da altri) e soprattutto il nostro diritto di non dire nulla su di noi (così come faremmo in un qualsiasi negozio, rifiutandoci di essere profilati). La proposta di revisione del Regolamenti eIDAS si muove esattamente in questa direzione, sia pure con i limiti che si è cercato di evidenziare e che è auspicabile siano superati.

b) Occorrerebbe riconoscere lo stato di persona giuridica da noi controllata a taluni identificatori (SEID, IMEI, Serial Number, ecc.) ed ai sistemi informatici attraverso i quali operiamo nelle reti (smartphone, tablet, PC)[42], per le stesse ragioni per cui si è riconosciuta la personalità giuridica alle associazioni, fondazioni e società, ossia per fare emergere meccanismi di

[42] R. GENGHINI, Digital New Deal: The Quest for a Natural Law in a Digital Society, cit., p. 207 ss.

traslazione degli effetti giuridici trasparenti e capaci di ingenerare legittimo affidamento e certezza delle relazioni giuridiche. Solo se gli strumenti informatici che generano il nostro UID sono sotto il nostro esclusivo controllo, l'identità (digitale) nel mondo informatico cesserà di essere una finzione giuridica, priva di ogni sostrato fenomenologico. Gli ordinamenti giuridici degli stati membri dell'Unione Europea conoscono (oltre alle anagrafi comunali) due istituzioni secolari che sarebbero in grado di fornire ai cittadini una vera identità digitale: sono i notai e le banche. Dal punto di vista della storia dell'identificazione, lo stato è l'ultimo arrivato e, nei 150 anni in cui si è immischiato nel "mestiere" di identificare le persone, non di rado lo ha fatto con finalità e risultati che non sono proprio commendevoli.

c) Il vigente Regolamento eIDAS ha fatto un primo passo nel senso di sottrarre l'identità spendibile on-line al preteso monopolio dello stato e nel senso di farla divenire un dato fenomenologicamente vero della transazione digitale. Purtroppo, nella sua attuale formulazione la proposta di revisione del Regolamento eIDAS, arretra in modo preoccupante, trasformando tutti i servizi elettronici di fiducia in servizi ancillari accessibili solo tramite il Wallet, di cui nel testo della legge manca, come visto, una adeguata definizione. Inoltre, l'applicazione pratica del Regolamento eIDAS (e la relativa proposta di revisione) sono influenzate dall'idea (superficiale ed errata) che l'unica "vera" identità sia il nostro profilo generato e gestito dall'anagrafe e dallo stato civile: tale errore di prospettiva determina il rischio grave che i Wallets diventino degli strumenti di controllo di massa, anche se questa non è certo la loro finalità, almeno nelle intenzioni della Commissione, del Consiglio e del Parlamento europei.

d) Occorre che gli *identity provider* eIDAS si facciano promotori di strumenti di autogenerazione ed autogestione dell'identità (come la blockchain, o gli smartphone) che si potrebbero definire "*freedom devices*" perché presentano alla rete l'immagine e l'idea di noi che noi ci scegliamo liberamente, e non il profilo che il gestore del dominio ci ha imposto per potere operare al suo interno, esponendoci ad una profilazione generalizzata e totale. La giurisprudenza comincia a muoversi in questa direzione: la Corte Suprema USA in due casi ha già deciso che gli smartphone sono protetti dall' habeas corpus[43] come se fossero parte di noi stessi.

e) I diritti inalienabili della persona nello spazio digitale vanno garantiti sempre ma solo ed esclusivamente a coloro che usano delle vere identità digitali. Significa che vanno riconosciuti solo ed esclusivamente alle persone fisiche identificate mediante l'identità da loro scelta (e non tramite un profilo

[43] Riley vs. California 573 U.S. 2014. e Carpenter v. United States, No. 16-402 585 US 2018.

imposto da un dominio), mentre non possono essere riconosciuti ad agenti informatici che non sono espressione di una identità liberamente scelta. Per comprendere ciò, occorre ricordare che gli attuali princìpi in materia di diritti inalienabili della persona non consentono la loro estensione automatica ad animali o robot. Soprattutto non consentono la loro applicazione a un soggetto che potrebbe essere umano, ma non è certo che sia così. Pertanto, se esistessero degli automi che sono la perfetta replica di un essere umano, non si applicherebbero ad essi come non si applicherebbero ad una scimmia particolarmente intelligente.

Nell'era dei social media è divenuto evidente che senza una vera identità (digitale), tutte le conquiste sociali, politiche ed economiche degli ultimi due secoli sono gravemente minacciate, perché quando il popolo cessa di essere una somma di individui responsabili, e torna ad essere una massa indistinta senza identità, inevitabilmente la politica torna ad essere repressiva e populistica, perché non si rivolge più ad una somma di individui (reali) ma ad una massa amorfa che non ha niente da perdere e neppure nulla da guadagnare perché composta da soggetti senza identità.

Purtroppo, di questo afflato di libertà nella proposta di revisione del Regolamento eIDAS non vi sono indicatori sufficienti. Essa non si coordina come dovrebbe il GDPR e neppure con le proposte di Digital Services Act e Digital Markets Act. Probabilmente alla base di ciò, vi è l'assunto che il Wallet di identità digitali sia uno strumento neutro: ma non è così, come visto. Il Wallet o migliora (anche solo marginalmente) lo status-quo, sotto il profilo dei diritti civili e della privacy, oppure diverrà funzionale ad una significativa loro compressione.

Seguendo i lavori del Parlamento Europeo e, per quanto possibile, del Consiglio, si può essere ragionevolmente ottimisti che le alte finalità della riforma, enunciate dalla Presidente dell'Unione Europea nel 2020, saranno rispecchiate nel testo finale del Regolamento: il lavoro delle Commissioni parlamentari ITRE, LIBE e ICOM sui punti evidenziati in questo contributo, è assai scrupoloso ed attento, per cui si può essere fiduciosi che ciò troverà adeguato riscontro nel testo che sarà licenziato dal Parlamento.