Dall'Identità Personale all'Identità Digitale

Se un cittadino, oggi, e indipendentemente dal suo utilizzo di Internet, volesse rinunciare al suo "essere digitale" gli sarebbe possibile? Quanta effettiva competenza ha un soggetto qualsiasi per decidere fino in fondo quando uscire da una rete digitale nella quale può entrare suo malgrado? La domanda nella sua banalità, apre di fatto scenari diversi e suscita molteplici riflessioni da parte degli addetti ai lavori. Le risposte, a loro volta, sono molte, spesso ancora abbozzate e rivelatrici della poca dimestichezza che si ha nel considerare il problema dell'identità digitale oltre la sua rappresentazione in termini di tecnologie usate per la gestione. È degli ultimi anni la consapevolezza che il tema è dei più delicati e necessita di un'analisi approfondita e multidisciplinare, tale da produrre risultati che possano essere condivisi e conosciuti dai proprietari delle informazioni che partecipano alla costruzione in rete di una loro identità per presentarsi ad altre identità con le quali intendono relazionarsi. Riflettere compiutamente sulle differenti implicazioni sottostanti ai molti punti di vista è una necessità se si vuole rispondere ad un bisogno ormai avvertito di trovare categorie idonee alla interpretazione dei cosiddetti diritti di cittadinanza digitale all'interno dei quali il diritto alla privacy è uno dei più rammentati.

Fare chiarezza su alcuni concetti che possono fin dall'inizio originare confusione all'interno di uno schema di riferimento in cui si intende muoverci è auspicabile. Asserire che il problema della identificazione in rete non si pone solo per Internet aiuta a decifrare l'ambito di applicazione delle regole tecnico giuridiche che man mano vanno delineandosi, dovendo essere comunque gestite attraverso la rete un numero sempre più elevato di relazioni tra cittadini e cittadini, tra cittadini ed imprese, tra cittadini, imprese e pubblica amministrazione.

Parlare di identificazione significa, nella prassi giuridica, riferirsi specificamente a persona fisica ed alle caratteristiche indispensabili e immutabili alle quali si riconduce una entità per differenziarla dalle altre che compongono l'insieme; ma significa anche assumere che un soggetto terzo ne effettui l'associazione in un documento che "a vista" dimostri ciò che dagli atti, in archivi appositamente costruiti e predisposti per rispondere a domande specifiche, risulta si debba dimostrare di essere in quel preciso momento. Tale documento indipendentemente dal supporto fisico che lo contiene diventa il *pass*, la chiave idonea ad aprire le porte fisiche o virtuali attraverso le quali si raggiungono i luoghi che, previa identificazione da parte del tenutario e certificatore dei dati, si è autorizzati a visitare. Il luogo in questo caso è da considerarsi come la metafora di ciò di cui abbiamo bisogno, informazioni, servizi e quant'altro possa rappresentare una risposta. L'identificazione rappresenta quindi la prima tappa di un procedimento che sfocia nell'autorizzare chi ne ha titolo – e solo lui – a fare o non fare ciò per cui lo stesso soggetto è stato prima identificato e successivamente autorizzato.

Come si può ben comprendere, la confusione interpretativa dei due momenti o addirittura la loro assimilazione rende difficile una corretta valutazione delle problematiche connesse alla gestione, in primo luogo, della identità personale, indipendentemente dalle regole di registrazione dei dati che la rappresentano, e secondariamente della identità digitale. Quest'ultima non è, per sua intrinseca natura, la versione digitale di quella fisica, anche se l'algoritmo che può rappresentarla permette l'accesso ai servizi offerti dalla rete, quando richiesto, così come il documento di identità permette, sempre che l'identificazione ne sia condizione indispensabile, l'ammissione alla presentazione della domanda per ricevere un servizio ad un *front-office* fisico. Un individuo può assumere in rete tutte le identità che la sua fantasia gli permette o può scegliere quella corrispondente alla sua reale posizione anagrafica attribuendosi ogniqualvolta i connotati che più lo soddisfano. Lo stesso individuo può altresì essere costretto a identificarsi o meglio autenticarsi con le regole tecniche e gli attributi personali stabiliti da leggi dello stato quando deve interfacciarsi con la PA. Comunque sia chi usa una o più *password* sa che al momento della richiesta di digitare lettere e numeri o di introdurre una carta elettronica lascia parte di sé o di quello che in quel momento e per quel servizio ha deciso di essere ed è ammesso che sia. Nella numerosità degli algoritmi usati, quando le regole gli appartengono, sta la convinzione di chi crede di poter salvare il proprio intero patrimonio informativo esponendo, di volta in volta, solo la quota di informazioni utili al soddisfacimento di uno specifico bisogno di cui la rete trasporta le soluzioni desiderate. In sostanza nel momento in cui attraverso un sistema si eseguono delle operazioni di autenticazione si condivide con il sistema un procedimento che pone alternative alla risposta ed è indifferente agli attributi di cui ci si vuole ornare a meno che la visibilità in termini di identificazione del richiedente espressa con connotati personali unici non sia prevista dalla normativa.

Il timore di essere espropriato di qualcosa che riconduce solo a lui medesimo accompagna la storia dell'uomo dal momento in cui, per l'evidente motivo di essere riconosciuto e accettato quale soggetto stanziale

in un determinato territorio, ha dovuto concedere informazioni uniche a chi a sua volta avrebbe dovuto registrare il suo passaggio come facente parte di quella comunità nella quale lo stesso uomo avrebbe accettati i doveri ed ottenuto i benefici collegati alla residenza. Con la gestione digitale delle informazioni sono cambiate la velocità con cui ciò che ci appartiene può essere diffuso e impropriamente utilizzato, e la pervasività della rete che trasporta in ogni dove i dati rendendo possibile la loro esposizione ed utilizzazione indipendentemente dalla volontà del titolare. Anche in condizione di archivi cartacei l'uso improprio di informazioni personali è possibile, ma i tempi con cui tale fatto può prodursi sono rallentati e coloro che ne possono avere la disponibilità hanno maggiori difficoltà ad un veloce trattamento. Tanti pezzi di una identità in rete e la possibilità che questi possano essere ricomposti in profili identificativi specifici, delicati nei contenuti e per i quali l'appropriazione indebita rappresenta un vero reato, costituiscono le paure che molti hanno quando volontariamente od obbligati dal fornitore del servizio devono digitare una *password* o introdurre una carta che la contiene.

Le regole attraverso le quali si entra e si esce da una banca dati come, per esempio, quella dell'anagrafe della popolazione, sono chiare e conosciute da parte del cittadino. Come è noto, le tracce del nostro essere stati qualcosa rimangono e servono a ricomporre la storia degli uomini singoli e delle comunità alle quali, a titolo diverso, sono appartenuti e attraverso le quali hanno transitato. Appare evidente che quando non si tratti di registrazioni obbligatorie indispensabili al riconoscimento di uno stato di diritto, il rilascio di informazioni personali, sotto qualsiasi forma, rientra in quelle attività compiute con qualche timore perché percepite dai più come un momento di espropriazione di qualcosa che appartiene ai diritti primari della persona. Nessuno, comunque, può immaginare un mondo in cui un soggetto fisico può essere cittadino digitale, con tutte le caratteristiche che gli permettono di formulare la propria identità come sintesi di quello che è nelle varie e innumerevoli attribuzioni che lo riguardano e quindi con elementi di riconoscimento oltre ai propri dati anagrafici, nonché rappresentabile, se lo vuole, da una identità biografica vera e propria, ed essere contemporaneamente anonimo quando quello che chiede alla rete è riferibile a se stesso. Quello che tutti ritengono indispensabile e irrinunciabile è che si possano rendere invisibili ad altri i legami tra il portatore di una istanza, qualunque essa sia, e l'erogatore del servizio, quando la richiesta comporta il trattamento di informazioni, nella fattispecie di dati sensibili così come definiti dalla normativa. Molti sanno che esistono le leggi, a partire dalla Costituzione, appositamente pensate per questa protezione, ma avvertono ugualmente la difficoltà ad ammettere di sentirsi completamente tutelati, stante la complicata e difficile dimostrazione che l'abuso può essere impedito.

Ciò che deve crescere, uscendo da fumose argomentazioni e da complicate disquisizioni tecnologiche, è la consapevolezza che la necessità di trovarsi ad assumere fisionomie digitali è oggi un fatto molto spesso non volontario ed inevitabile, in quanto la rappresentazione delle soluzioni proposte a soddisfacimento di bisogni reali non contempla altra soluzione. Dalla pragmatica osservazione della nuova realtà fattuale da parte del cittadino deve discendere la ulteriore accettazione del dovere di condividere con la comunità digitale di riferimento gli strumenti, più o meno complessi, che vengono messi a disposizione dalla tecnologia, pretendendo che gli stessi siano accompagnati nell'uso da una normativa di riferimento che ne abiliti l'ufficialità ai fini della salvaguardia dei diritti degli utilizzatori attivi o passivi della rete.

Dalle argomentazioni sin qui svolte, e con specifico riferimento alla domanda posta all'inizio, si potrebbe avanzare l'ipotesi che l'uomo del terzo millennio, di fronte alla questione dell'identità digitale riferita alle tematiche connesse alla soddisfazione del diritto alla *privacy*, può trovarsi ad analizzare il suo essere cittadino all'interno di due diversi ambiti relazionali semplificabili nelle descrizioni di seguito abbozzate.

Il cittadino portato nella rete suo malgrado, in quanto cittadino di uno Stato, inteso nella accezione di tutta la PA, che sceglie di sostituire, approfittando di quanto oggi è possibile ottenere dalle ICT, i suoi sistemi informativi con sistemi interamente digitali, all'interno però di un sistema di *governance* del processo innovativo che prevede una trasformazione graduale anche del suo sistema ordinamentale in modo da codificare ciò che è ammesso e ciò che è negato. In questo caso la manifestazione di volontà del cittadino di essere o non essere soggetto digitale è espressa nei vari passaggi previsti dalla norma che accompagna il procedimento digitale cui è comunque obbligato a rispondere per essere o non essere qualcosa. In questo contesto non esiste alternativa e quindi potremmo dire che si diventa digitali nel momento in cui si diventa cittadini di una tale realtà statuale. Fino a che esisterà invece la possibilità di rivolgersi ad un *front-office* fisico, la scelta potrà essere fra il pensare di tutelarsi dando o chiedendo a voce certe informazioni ad uno specifico addetto, o il credere che i contatti *on-line* con la PA non sono meno sicuri, visto che – comunque esso sia acquisito – il dato è ormai gestito digitalmente e quindi soggetto alla velocità di trasferimento e trattamento in ogni dove a cui prima è stato accennato.

La tecnologia è oggi il motore per una rapidissima evoluzione verso soluzioni sempre più spinte nella ricerca di dematerializzare i procedimenti burocratici sottostanti ai rapporti tra cittadino e PA, per la qualcosa il cittadino è uno spettatore utente più o meno interessato e accondiscendente al cambiamento che gli viene proposto. Quando il passaggio alla versione completamente digitale di tali procedimenti sarà avvenuto, e meglio sarebbe se tale passaggio fosse accompagnato da consenso e accrescimento culturale, la possibilità per il cittadino di sottrarsi del tutto al cambiamento verrà meno, giacché lo stato di necessità lo obbligherà a certe operazioni derivanti dal suo stato di cittadinanza.

A questo livello il problema dell'identità in rete deve, come di fatto sta lentamente avvenendo, essere gestita con regole e tecnologie definite e ascrivibili a strumenti

certi che riferiscono a sistemi pubblici appositamente normati. La persona fisica a cui viene associata una sua versione digitale sarà tanto più tranquilla quanto più avrà fiducia nella PA alla quale digitalmente si relaziona. La fiducia verso chi tiene i dati è però un presupposto della tranquillità anche prima di arrivare al momento della autenticazione in rete, e precisamente già quando gli archivi digitali vengono organizzati per i successivi trattamenti. Il fatto che possano sussistere dubbi sulla corretta tenuta delle banche dati o che il dato possa essere usato impropriamente, non può essere ritenuto problematico solo nel contesto digitale. Leggere le eventuali difficoltà dell'utenza nell'uso di sistemi digitali di identificazione pensando solo a ciò potrebbe infatti risultare fuorviante e riduttivo.

Seguendo questo ragionamento si può affermare che in ambito pubblico il cittadino deve poter stare nel digitale con la convinzione di essere protetto nella sua *persona* e quindi con le sicurezze che egli si aspetta vengano attivate a salvaguardia dei suoi diritti fondamentali, digitali e non. Ai fini del ragionamento sin qui svolto appare utile considerare inoltre che il tema della fiducia si riferisce alla PA in tutte le sue articolazioni e a chi la stessa PA delega le sue attività gestionali oltre che a tutti quei fornitori di servizi digitali pubblici e privati ai quali l'uomo di oggi ormai quotidianamente si interfaccia.

La seconda fattispecie in cui può riconoscersi l'umanità del duemila è rappresentata da colui che con manifestazioni di volontà afferenti alla propria sfera privata sceglie di utilizzare servizi presenti in rete nelle più diverse e sofisticate tecnologie, aderendo a regole tecniche che altri soggetti privati, pur condizionati da norme di valore generale, gestiscono per il funzionamento della rete stessa. In questo caso il tema della volontarietà ad acquisire caratteristiche o meglio essenze digitali assume altri significati per le conseguenze che possono scaturire dall'accettazione a stare in rete a quelle condizioni. La decisione di essere o non essere digitale in certi contesti è completamente a capo del soggetto che compie la scelta. Conoscere le regole è un suo dovere per poter poi decidere i modi con cui stare ed usare le potenzialità della rete nonché quelle per relazionare con gli altri soggetti della comunità. A tale proposito potrebbe dirsi che la tutela dei diritti deriva dalla norma generale, ma la controparte con la quale potrebbe verificarsi il contenzioso non ha sempre, per motivi oggettivi o per scelta, quella riconoscibilità alla quale il soggetto pubblico, PA o chi in quel momento la rappresenta, è obbligato a dare consistenza nel momento che gli viene richiesto. Se in rete e con riferimento alla comunità di appartenenza si ha più fiducia di affidare le credenziali ad un soggetto pubblico o privato dipende, molto probabilmente dalla percezione che il cittadino ha del livello di maturità democratica espresso da chi quella comunità rappresenta e di quanto il senso democratico è presente nel vissuto quotidiano dei suoi interlocutori reali.

Importante appare, in entrambi i casi sommariamente descritti, la possibilità di poter disporre da parte dell'uomo del terzo millennio delle conoscenze necessarie alla decodifica, in un linguaggio naturale, dei passaggi che gli vengono imposti dal sistema nella costruzione del procedimento digitale, qualunque esso sia, e della comprensione del valore, in termini di bene personale, che assumono in rete le informazioni che gli permettono la navigazione e i diversi livelli di accesso.

Certo è che la complessità dei sistemi poco garantisce chi non è esperto e, a maggior ragione, la sensazione di trovarsi impotenti di fronte ad un uso improprio di quanto scorre in rete può spingere a resistere al nuovo modo di essere. La scarsa conoscenza delle potenzialità dello strumento può produrre effetti quali la rinuncia all'uso e all'apprendimento dello stesso da una parte o, alternativamente, la richiesta di servizi formativi dall'altra. Il secondo comportamento è proprio di chi vuole possedere, come consumatore di nuovi beni, quanto serve in termini di patrimonio informativo per poter consapevolmente e in assoluta libertà gestire il proprio essere digitale, avendo conoscenza di quelli che sono i veri rischi che corre in rete rispetto alla propria *privacy* e rivendicando altresì il principio che la libertà all'accesso non possa essere limitata dalla convinzione di non poter esercitare con certezza il diritto ad uscire con cancellazione certa delle sue credenziali quando lo desideri. Sentirsi completamente nelle mani di altri per una cancellazione, o addirittura comprendere che con quello che di noi resta in rete si possa costruire, al bisogno, un altro soggetto che ci assomiglia e che può sostituirci nelle responsabilità che derivano dalle relazioni, fa aumentare la richiesta di sicurezza, esprimibile con ulteriori difficoltà tecnologiche da frapporre fra l'utilizzatore e gli altri cui intende nascondersi.

Il “consumatore evoluto” di Internet, frequentatore di siti e portali che effettua transazioni *on-line* con o senza pagamenti, cosciente di quali possano essere i punti deboli di tutto il sistema, sa che le fasi da attraversare vanno, a seconda del servizio che si chiede, dall’identificazione all’autenticazione e all’autorizzazione, come più volte sin qui evidenziato, ed ha la capacità di decidere come stare nella comunità telematica. Conosce il rischio e ne accetta le conseguenze. Per un consumatore meno o per niente esperto la percezione di dipendere completamente dai corretti comportamenti di altri soggetti non agevola l'uso, se degli altri non si ha totale e piena fiducia.

A conclusione di queste brevi riflessioni può essere azzardata l'ipotesi che, vista l'impossibilità di potersi sottrarre a questo nuovo modo di essere, più o meno volontariamente acquisito, l'uomo di questo secolo, per il problema di cui si discute, ha bisogno di essere rassicurato: questo può avvenire attraverso la messa a punto di regole idonee, conosciute e partecipate (come quelle, per esempio, inerenti la distruzione dei dati dopo l'uso o l'immediata individuazione dei responsabili del trattamento), ma anche attraverso la definizione di un sistema di tutele, con riferimento alle tecnologie usate, tale per cui all'utente è dato conto di quello che realmente avviene quando esercita un suo diritto attraverso i sistemi digitali. Questi, del resto, fanno ormai parte, anche suo malgrado, di un pacchetto di strumenti dai quali non può più prescindere per stare nello spazio virtuale cui corrisponde il mondo in cui vive.