

XXIII Convegno SISP – Società Italiana di Scienza Politica
Roma, Facoltà di Scienze Politiche LUISS Guido Carli
17-19 settembre 2009

Sezione: **Comunicazione Politica**
Panel: **Diritti di cittadinanza e nuovi ambienti digitali**
Chairs: **Francesco Amoretti e Claudia Padovani**
Discussants: **Stefano Rodotà**

SICUREZZA PUBBLICA E CITTADINANZA IN RETE

Gianpasquale Preite
Università degli Studi di Foggia
g.preite@unifg.it

Abstract

L'utilizzo di internet su scala globale, la diffusione delle ICTs¹ e le specificità funzionali dei nuovi media aprono scenari di riflessione che coinvolgono modelli socio-politici, in ordine agli effetti prodotti sulle forme di partecipazione democratica, sulla sicurezza pubblica e sulla privacy, inducendo un nuovo modo di intendere le relazioni interpersonali e interistituzionali caratterizzate dallo scambio di informazioni e conoscenza.

Il valore dell'informazione è, infatti, lo snodo dal quale valutare politiche pubbliche ed aspettative giuridiche in presenza di un trattamento del patrimonio informativo veicolato con elevata generalizzazione dai nuovi media. Si rileva, dunque, che se da un lato lo scambio di conoscenza assume un ruolo strategico nella gestione del cambiamento, dall'altro rimanda alla necessità di ripensare le condizioni che definiscono il valore dell'informazione digitale e che sono alla base del bilanciamento tra aspettative giuridiche, diritti fondamentali, pratiche di sorveglianza e dispositivi di controllo.

Si tratta di una prospettiva che assume particolare rilievo se analizzata in termini di sicurezza pubblica. In particolare, si evidenzia che le attuali esigenze di protezione, sicurezza e prevenzione sono perseguibili solo attraverso tecniche e dispositivi di controllo in rete che superano i limiti delle tradizionali metodologie di riconoscimento ed in cui il bilanciamento tra sicurezza e privacy richiede la ricerca di un equilibrio dinamico tra esigenze contrapposte.

¹ Le ICTs (information and communication technology), rappresentano l'insieme integrato delle tecnologie che consentono di elaborare e comunicare l'informazione attraverso mezzi digitali, i c.d. nuovi media, che sono strumenti interattivi composti da un codice digitale e che hanno in comune l'uso dei sistemi informatici.

Con queste premesse, l'obiettivo del presente paper è quello analizzare le condizioni per la realizzazione del bilanciamento sicurezza/privacy nella Società dell'informazione, in una prospettiva di compatibilità con i diritti dell'era digitale. In particolare, il contributo si propone di presentare un'analisi ricognitiva che dal diritto di *habeas corpus* della tradizionale cultura giuridica europea, perviene alla garanzia di *habeas data*, attraverso il processo di autodeterminazione informativa in rete.

1. Nuovi media e ICTs: traiettorie evolutive nella gestione dell'informazione e della conoscenza

L'era in cui viviamo e l'ambiente in cui opera il sistema della politica, sono fortemente condizionati dagli effetti generati dall'impiego di media digitali, il cui sviluppo ha determinato un mutamento radicale nel modo stesso di concepire il mondo, le relazioni e i rapporti interpersonali, la produzione e lo scambio di informazioni (Gamaleri 1998), incidendo sugli elementi costitutivi della società e sul senso di comunicazione del sapere all'interno di un quadro intellettuale unico (Castells 2002). Tali effetti assumono importanza nella ricostruzione temporale-concettuale che porta alla definizione di società dell'informazione, i cui prodromi risalgono alla seconda metà del novecento, periodo in cui l'idea di "società post-industriale" si colloca al centro di un complesso dibattito attento ad approfondire lo studio del rapporto tra tecnologie informatiche e informazione/conoscenza, e dal quale ha tratto origine un nuovo paradigma che riconosce gli effetti di reciprocità tra i due aspetti, in altri termini, si sostiene che le tecnologie agiscono sull'informazione e quest'ultima sulle tecnologie, con effetti in tutti gli ambiti del sapere (Touraine 1969; Bell 1974; Stonier 1983; Lyon 1991; Castells 2000).

In Europa, la definizione di Società dell'informazione trova piena formalizzazione nel 1994, con il *Bangemann Report* dal titolo *Europe and the Global Information Society* da cui nasce e si sviluppa una nuova filosofia gestionale che attribuisce un ruolo fondamentale all'approccio di tipo integrato nell'utilizzo delle ICTs per l'innovazione, lo sviluppo, l'integrazione, la conoscenza, l'accesso, l'inclusione, la sicurezza degli attori sociali coinvolti (Downey McGuigan 1999; Padovani, Nesti 2003; Servaes 2003; Goodman 2006).

In forza di questa eredità, l'attuale sistema della politica si considera "informazionale" nella misura in cui l'organizzazione, la struttura decisionale e il funzionamento degli apparati, dipendono dalla capacità del sistema di generare e applicare in maniera ricorsiva e con efficienza "informazione basata sulla conoscenza"; in altri termini, capacità del sistema di produrre e riprodurre le strutture e gli elementi di cui è composto rappresentando il risultato di un processo in cui la conclusione di una

operazione è la condizione di possibilità di un'altra operazione (Luhmann, De Giorgi 1994). Tale dimensione "informazionale" è alla base della velocità di scambio dei flussi informativi e si traduce nel modello che Castells (2002) definisce "Società in rete" ed in cui le ICTs, rappresentano l'esito finale di un insieme di innovazioni scientifiche e tecnologiche. Tuttavia, la centralità della nuova rivoluzione tecnologica non è attribuibile alla conoscenza e all'informazione in quanto tali, ma alla loro applicazione a dispositivi che generano conoscenza e che producono la possibilità di percepire il senso di ciò che viene comunicato. La produzione e riproduzione della conoscenza è un nuovo valore dello scambio sociale, l'espressione di una socialità attiva che si combina con la dimensione della soggettività, la conoscenza è, dunque, un concetto che si ridefinisce a partire dal suo valore d'uso, e che si declina in modi differenti, si seleziona e si contestualizza affinando la capacità selettiva in relazione all'esperienza.

Il sistema politico ha riconosciuto, nel corso di quest'ultimo decennio, l'importanza dell'informazione e della conoscenza in uno scenario sociale multidisciplinare e multisistemico non in contrapposizione rispetto al passato, ma alla ricerca di nuovi modelli di riferimento.

Inoltre, come ampiamente mostrato dalla sociologia della scienza e della tecnologia (Pinch et Al. 1987; Pickering 2001), ogni tecnologia (e le ICTs in particolare), partecipa in modo attivo alla costruzione dell'ambiente organizzativo quotidiano. Le risorse per l'innovazione non risiedono, quindi, all'interno della singola organizzazione, ma sono rintracciabili negli interstizi in cui si incontrano saperi e modalità organizzative eterogenee (Powell 1990). Sempre più spesso le ICTs si configurano quali tecnologie di mediazione tra organizzazioni ed interlocutori privati ed istituzionali (cittadino/Stato). Ne consegue, che i nuovi media assumono rilevanza non solo come strumenti che permettono agli utenti/cittadini, tendenzialmente isolati, di accedere ad una varietà di risorse informative, ma anche quali tecnologie sociali che permettono di condividere e negoziare nuove forme di conoscenza e relazione (Castells 2000). L'interrogativo centrale ruota attorno a come il sistema della politica sfrutterà nuovi media e ICTs, nell'immediato futuro, per attivare sistemi di conoscenza distribuita in diversi contesti e dinamiche organizzative, all'interno di uno schema teorico che interpreta conoscenza e apprendimento quali processi sociali.

2. Sicurezza e diritti fondamentali nella società dell'informazione

In tema di sicurezza pubblica, il ricorso alle ICTs ha avuto un'influenza fondamentale sui meccanismi di controllo sociale. L'impiego di tecnologie avanzate copre la gamma che va dalla verifica delle identità, all'autenticazione fisica e fisiologica, alla sorveglianza elettronica, alla gestione e al coordinamento delle stesse attività sociali, descrivendo un

fenomeno che in termini foucaultiani (Foucault 1977/1978; 1978/1979) si potrebbe definire “statalizzazione del biologico” come risultato dell’esercizio di due forme di potere: biopotere e biopolitica.

Dagli anni settanta del secolo scorso si è assistito ad un rapido passaggio dalla società “disciplinare e del controllo” descritta da Foucault, alla società “informazionale”, ma è pur vero che la sorveglianza è una delle caratteristiche fondamentali della società dell’informazione che investe non soltanto il corpo biologico, la fisicità della persona con la relativa sfera di libertà (*habeas corpus*), ma anche la sua dimensione elettronica, digitale (*habeas data*). Pochi dubbi esistono riguardo al fatto che la sorveglianza sia oggi da considerare come il mezzo essenziale dell’ordine e della gestione sociale: le società dell’informazione sono società sorvegliate (Lyon 2002).

Una delle più importanti affermazioni degli ultimi anni è “che ogni tecnologia è un’estensione di noi stessi” (McLuhan 1999). La società dell’informazione mette in gioco scelte sociali e politiche che in genere si presentano di fronte a cittadini quali possibilità frutto dell’impiego di determinati servizi digitali (Van Dijk 2002) e permettono un’interazione diretta tra le parti; ciò comporta, da un lato maggiore interazione e partecipazione, ma dall’altro rischi di controllo e d’incursioni nella sfera dei diritti della personalità. A ciò si aggiunge una nuova problematica che nasce dall’esigenza di estendere anche al mondo virtuale quell’insieme di attività dirette a uniformare la condotta degli individui con l’obiettivo di far rispettare le norme e le aspettative del gruppo, inoltre, attraverso i nuovi media si entra in una logica di conquista di senso comune ottenendo il consenso da parte della società (Ragnedda 2006; 2008).

La questione della cittadinanza in rete implica un elevato livello di complessità riguardo alla difficoltà di specificare i diritti che ne derivano rispetto a un numero sempre maggiore di situazioni ed eventi connessi all’utilizzo dei nuovi media nelle relazioni interpersonali e interistituzionali. In tale contesto, l’espressione “diritti fondamentali” è più precisa rispetto a quella di “diritti umani” e più adatta per comprendere tanto i fondamenti etici quanto le componenti giuridiche dei diritti senza incorrere nel riduzionismo giusnaturalista o in quello positivista. Nei diritti si celebra una sorta di straordinario equilibrio tra tecniche di controllo, prestazioni funzionali, forme giuridiche, consenso morale, aspettative rilevanti; i diritti fondamentali esprimono allo stesso tempo una moralità e una giuridicità fondamentale (Peces-Barba 1993, 23-24), ma la dogmatica dei diritti fondamentali non è sufficiente a risolvere le problematiche legate al tema in questione. «*I diritti nascono quando devono e possono nascere*», cioè quando si formano nuove pretese in vari ambiti del sapere (Bobbio 1990), non sono “diritti umani eterni”, ma istituzioni sociali che si affermano e si sviluppano in una specifica fase dell’evoluzione sociale e che si sostanziano in un complesso di reali aspettative di comportamento, il materiale vivo su cui si esercitano le opzioni di fondo della comunicazione etica e politica

(Luhmann 2002, 11). Garanzie e tutela definite assolute, in realtà sono strettamente connesse al modo di evolvere della società, evidenziando il requisito storico piuttosto che naturale dei diritti fondamentali. In tal senso emerge l'esigenza di specificare i diritti nella forma di istanze esterne al sistema che processano all'interno operazioni per «*affrontare la complessità sociale, consentendo ai sistemi di mantenere in primo piano e di tutelare aspettative di comportamento che hanno radici altrove*», si configura un diritto fondamentale che spetta al cittadino e si rivolge allo stato come soggetto obbligato, risolvendo la complessità nella distinzione tra diritto e non diritto. Purché il diritto fondamentale esista e valga nella misura prevista, il cittadino è titolare del diritto e lo stato è corrispondentemente obbligato; oltre questo limite lo stato può agire liberamente e il cittadino deve accettarne le conseguenze (Luhmann 2002, 301).

A livello politico e filosofico-giuridico si è dibattuto a lungo circa la ripartizione generazionale dei diritti, dove nel termine “generazioni” si ravvisa un processo in continuo sviluppo, sempre più specializzato (Bobbio 1990) e che, dopo la Dichiarazione universale dei diritti umani, ha portato all'affermazione di una nuova generazione di diritti relativi al campo delle manipolazioni genetiche, della bioetica, delle nuove tecnologie dell'informazione e della comunicazione, ossia diritti aventi oggetti o contenuti immateriali che tendono a realizzare uno sviluppo della persona in quanto tale in assenza di ogni forma di mediazione da parte del potere politico, fondati, dunque, direttamente sulla individualità in sé considerata (Barcellona 2005, 152).

Oggi, nella prassi giuridica della maggior parte delle Corti costituzionali europee, la questione dei nuovi diritti è affrontata attraverso la tecnica del bilanciamento o ponderazione, impiegata sia per risolvere problemi di costituzionalità che emergono dal contrasto tra diritti o interessi diversi, sia per trattare interessi che non hanno uno specifico riconoscimento in Costituzione (Alexy 2002). Nel linguaggio costituzionale è corretto riferirsi ai nuovi diritti per indicare l'assenza di una specifica disciplina costituzionale.

In una ipotetica matrice, atta a rappresentare livelli di “opportunità” e “minacce” legate ai nuovi media ed alle applicazioni ICTs nella società dell'informazione, si rilevano evidenti vantaggi che attraggono le nuove tecnologie nell'area dei valori economici, ma di contro emergono minacce connesse all'area dei diritti, che potrebbero tradursi in lesioni dei diritti e delle libertà fondamentali, con spazi per la discriminazione, la stigmatizzazione e la sopraffazione burocratica (Rodotà, 2004). In particolare, si rileva la necessità che all'evoluzione tecnologica delle fattispecie criminose debba corrispondere la definizione di nuovi livelli di tutela della persona. Ciò non significa affermare la nascita di nuovi diritti universali, ma di rivisitare le categorie giuridiche esistenti in direzione della tutela di fattispecie più ampie e complesse.

I diritti che ridefiniscono l'integrità stessa della persona, comportano, pertanto, una riflessione finalizzata alla rivisitazione della distinzione tra diritto di *habeas corpus* delle Costituzioni più antiche, e diritto di *habeas data*, su cui si fondano le Costituzioni più giovani². In questa direzione si colloca la valutazione in ambito politico dell'esistenza o meno di una corrispondenza delle regole costituzionali vigenti alle fattispecie giuridiche che emergono nella società dell'informazione. In altri termini, il problema che il legislatore deve affrontare è la "dilatazione" del concetto di libertà personale, intesa come "autonomia e disponibilità della propria persona" in virtù del fatto che la tutela del corpo fisico è, oggi, anche tutela delle informazioni personali che lo riguardano (a titolo esemplificativo il riferimento è al diritto alla privacy, al diritto di accesso, diritto all'oblio). In questo passaggio, la cultura giuridica tradizionale si scontra con l'affermarsi di una società dell'informazione in cui viene meno la corrispondenza piena e oggettiva ai principi costituzionali vigenti.

In Italia, così come in molti altri stati dell'Unione europea, i diritti della sfera individuale assumono valenza costituzionale con una *tecnica a spirale*, che inizia con l'*habeas corpus* (art. 13 Cost. sulla libertà della persona fisica), ossia con la garanzia della persona e dei beni fisicamente connessi ad essa, estendendosi all'ambito spaziale immediatamente circostante e così via in maniera ricorsiva, creando una continuità nella tutela della sfera individuale che porta la libertà personale a saldarsi con altri diritti sanciti dalla Costituzione (Bin, Pitruzzella 2001, 481-490), in tal modo se da un lato si rafforza e si completa la garanzia complessiva dei diritti individuali, dall'altro si assiste ad una variazione della tutela che tende a dilatarsi all'aumento della distanza dal punto di origine. Tale constatazione ha indotto l'Autorità Garante per la protezione dei dati personali a richiedere, sul piano politico-legislativo, interventi specifici per un rapido passaggio alla garanzia costituzionale di *habeas data*, in funzione della quale le persone hanno il diritto di pretendere che l'immagine che gli altri hanno di esse corrisponda all'esatta realtà (Acuña 2002, 1928), rientrano: *il diritto di protezione dei dati* (come tutela dei diversi diritti della persona che possono essere lesi dai gestori dei dati personali); *il diritto alla protezione dei dati personali* (come potere dell'individuo ad ottenere dalle pubbliche autorità, la difesa di quei diritti violati o minacciati dall'accesso, trasmissione, dalla cessione, ecc. dei propri dati personali); *la libertà d'informazione* (intesa come diritto alla autodeterminazione informativa della persona, ossia il diritto a determinare il quando, il come e il quantum di una informazione personale oggetto di comunicazione ai terzi); *la libertà informatica* (come garanzia personale a conoscere e accedere alle informazioni personali esistenti nelle banche dati, in formato elettronico, a controllare il loro

² La garanzia costituzionale di *habeas data* è presente nelle Carte costituzionali dei Paesi africani, degli ex "Paesi satellite" dell'Europa dell'est ed in particolare dell'America latina, che si caratterizzano per le più rilevanti novità in tema di garanzie costituzionali

contenuto e quindi a poterle modificare in caso di inesattezza o indebita archiviazione o trattamento, nonché a decidere sulla loro circolazione o trasmissione).

Parallelamente, si è innescato, in questi ultimi anni, un ulteriore dibattito socio politico sul rapporto diritto a internet e cittadinanza in rete, che ha portato alla proposta di redazione di una Carta dei diritti contenente principi, regole, codici deontologici, intese internazionali in grado di mantenere alla rete il suo carattere di infinito spazio di libertà (Rodotà 2005, 118), orientare l'inclusione in internet, lo sviluppo e la partecipazione democratica, arginare i fenomeni di prevaricazione, regolare lo spazio dello scambio economico, tutelare le regole del mercato e lo spazio della concorrenza (*Internet Bill of Right*, Rio 2007).

3. *Le problematiche connesse all'identità digitale e la questione della privacy in rete*

Nel corso dell'ultimo decennio un'ampia letteratura ha analizzato le forze di varia natura (politica, economica, sociale, tecnologica, istituzionale) che hanno influito sul processo di cambiamento dei rapporti interpersonali e interistituzionali che si svolgono in rete, delineando una morfologia evolutiva che corrisponde ad un diverso utilizzo dello spazio e del tempo.

Il terreno di analisi è, dunque, un "dominio" di interazioni in cui non è possibile prescindere dalla comprensione delle forme e delle caratteristiche che descrivono l'identità digitale e che impongono di affrontare la delicata questione dei livelli di vulnerabilità generati sia da fattori endogeni - a differenza di quanto possiamo fare con il nostro corpo fisico possiamo rapidamente creare un doppio elettronico (Rodotà, 2005, 114) - sia da fattori esogeni, cioè comportamenti qualificabili come attacchi esterni. Nell'ambiente digitale prende forma un principio di autodeterminazione informatica (e informativa) che, riducendosi da tensione di "affermazione" a sforzo di "negazione della esclusività altrui", assume il significato di tentativo infruttuoso di preservare ciò che di più caro rimane: il feticcio di una libera volontà (Frosini 1991, 115). Non potendo "affermare se stesso", il soggetto non può fare altro che "limitare gli influssi esterni", riducendone la portata ad un livello accettabile.

Il cittadino che si muove tra i servizi in rete non deve più identificarsi con i suoi dati anagrafici, ma con username e password. Sono questi i suoi codici di accesso, gli elementi che lo identificano individualmente, e che consentono di interpretare, soddisfare e memorizzare le sue richieste.

Inoltre, la gestione delle attività in rete, consente l'utilizzo di identità/profilo differenti, che facilmente possono generare confusione circa l'identità dell'utente e che sono celate dietro codici che racchiudono un valore molto elevato per l'utente.

La dematerializzazione del concetto di identità e di identificazione della persona porta con sé rinnovate esigenze di sicurezza e di tutela dei dati personali, non più esclusivamente a livello nazionale, ma globale, per contrastare il furto della identità digitale, la sua compromissione, il suo abuso (Crescentini 2007), tenuto conto che la sovrapposizione della vita sociale in rete a quella reale, è diventata la dimensione ideale per lo sviluppo dei *computers crimes* (Limone 1999).

La disamina degli attacchi che hanno come obiettivo di fondo quello del furto dell'identità digitale, rileva una serie di fenomeni che riguardano in maniera diretta l'identità della persona nel suo rapporto con la rete, tra i più interessanti si segnala l'appartenenza ai social network³, cioè reti sociali che connettono fra loro persone sulla base di legami tra i più svariati, quali vincoli di amicizia, parentela, lavoro, interessi di ogni tipo. Tali legami creano delle comunità virtuali delle quali l'utente può entrare a far parte costruendo un profilo personale corredato da una serie, talvolta anche molto ampia, di informazioni private: dai dati anagrafici all'indirizzo e-mail, passando per le proprie esperienze professionali, i propri interessi, le opinioni politiche, culturali, religiose, ecc. Quando l'utente decide di partecipare allo spazio sociale in rete si spoglia della sua fisicità ed utilizza la sua identità digitale, spesso modellata sulla base delle informazioni che di sé ha scelto di mettere in gioco: viene così sciolto, o fortemente allentato, il vincolo tra nome, corpo e identità (Rodotà 2006, 76).

La questione più controversa e delicata è rappresentata dal fatto che, nella maggior parte dei casi, le informazioni personali pubblicate attraverso la partecipazione a social network, sono frutto dell'iniziativa degli stessi utenti, trovano il loro consenso e la conseguente autorizzazione al trattamento dei dati immessi. Una questione, quest'ultima, che è stata sollevata dal Gruppo di lavoro internazionale sulla protezione dei dati nelle telecomunicazioni, che parla di una nuova generazione di utenti, la generazione cresciuta con internet, "indigeni digitali" che hanno sviluppato approcci del tutto peculiari rispetto all'utilizzo dei servizi in rete e, che essendo in buona parte adolescenti, sono probabilmente più disposti a mettere a rischio la propria privacy rispetto a coloro che hanno qualche anno in più e che rappresentano gli "immigrati digitali"⁴. A questa serie di considerazioni si aggiunge il pericolo di utilizzo improprio dei profili-utente da parte di soggetti terzi.

In linea generale, il Gruppo di lavoro dimostra di nutrire particolari preoccupazioni in merito al rischio del furto d'identità causato dalla

³ Un servizio di *social network* (rete sociale) consiste nella creazione e nel controllo di reti sociali on-line destinate a comunità di soggetti che condividono determinati interessi e attività, ovvero intendono esplorare gli interessi e le attività di altri soggetti, necessariamente attraverso l'impiego di applicazioni software.

⁴ In argomento: v. *Memorandum di Roma*, Rapporto e Linee-Guida in materia di privacy nei servizi di *social network*, adottato dal Gruppo di lavoro internazionale sulla protezione dei dati nelle comunicazioni, Roma, 3-4 marzo 2008.

disponibilità diffusa di dati personali contenuti nei profili-utente, e all'abuso di tali profili da parte di soggetti terzi non autorizzati.

A tal proposito, si rende opportuna una disamina delle peculiarità connesse ai dati e alle informazioni della persona.

La protezione dei dati personali rappresenta una particolare forma di tutela della privacy, positivizzata in normative legali *ad hoc*. La tutela di tale settore di nicchia, assolve ad una funzione di sostegno per la protezione del più ampio diritto alla privacy. Il diritto alla protezione dei dati assicura al cittadino il diritto di disporre dei propri dati relativi alla sua persona, che nella società dell'informazione assumono un valore esponenziale in ordine alle possibilità di raccolta, elaborazione, trattamento e conservazione. Tale nozione si sviluppa nei primi anni settanta del secolo scorso, quale nuova tutela comparata alla prima forma di diritto alla personalità.

Oggi, la relazione tra privacy e sicurezza genera un considerevole impiego delle ICTs per la tutela dei luoghi di lavoro, della proprietà e dei beni privati contro azioni criminose e, dopo gli attentati dell'11 settembre 2001, la protezione generalizzata (anche in Europa) di aree pubbliche, luoghi di aggregazione e luoghi di socializzazione in rete, contro azioni terroristiche.

A questa forte pretesa di sicurezza non corrisponde, tuttavia, un'adeguata visibilità dei livelli di invasività sulla sfera privata della persona. Appare evidente, dunque, che il bilanciamento tra sicurezza e diritti di *habeas data* è una questione complessa che richiede la ricerca di un equilibrio dinamico capace di contemperare esigenze contrapposte ed in continua evoluzione. A metodologie, tecniche e tecnologie di controllo, sorveglianza, monitoraggio e trattamento dei dati e delle informazioni digitali sempre più raffinate si contrappongono, infatti, aspetti sempre più delicati che investono la sfera privata degli individui, utenti della rete.

Infatti, le informazioni private di ogni singolo individuo circolano quotidianamente in molteplici attività. Si pensi alla corrispondenza elettronica, ai pagamenti con carte di credito e di debito, agli accessi in internet, alle telefonate, solo per citare alcuni esempi: si tratta di azioni di *routine*, che tuttavia lasciano una traccia "elettronica" indelebile nelle banche dati degli apparati che gestiscono il servizio e offrono una radiografia permanente dei rapporti, delle relazioni, delle scelte, dei gusti (anche sessuali), delle preferenze e dei movimenti fisici sul territorio di ogni individuo. Le tecnologie informatiche offrono numerosi vantaggi attratti nell'area dei valori economici ma rappresentano una sfida continua a vecchi diritti, che rischia di tradursi, nel tempo, in una potenziale violazione della dignità umana, dei diritti e delle libertà fondamentali, con spazi per la discriminazione, la stigmatizzazione e la sopraffazione burocratica (Rodotà, 2004). La tutela dei dati è *un diritto fondamentale della persona, una componente essenziale della nuova cittadinanza*, come si evince dall'art. 8 della *Carta dei diritti fondamentali dell'Unione Europea*.

Non vi è dubbio che il valore della privacy debba essere opportunamente controbilanciato con quello della sicurezza, ma a tutela dello stesso concetto di democrazia è importante che le ragioni della sicurezza non prevalgano incondizionatamente sui diritti fondamentali.

In Italia, il primo approccio di indirizzo politico-normativo è riconducibile all'attività dell'Autorità Garante per la protezione dei dati personali, concentrata sull'analisi dei "limiti" e degli "spazi" di utilizzo dei dati personali, sensibili, biometrici e genetici in tutti gli ambiti, non permettendo l'utilizzo metodologie di verifica invasive, come nel caso del riconoscimento biometrico (riservandone l'utilizzo in limitati casi dove il diritto alla pubblica sicurezza prevale sul diritto personale come il controllo antiterroristico, l'accesso ad aree riservate, a luoghi in cui sono custoditi documenti segreti o materiali pericolosi, ecc.).

Sul fronte europeo, il Gruppo di lavoro che ha coinvolto le Autorità garanti dei paesi membri, ha prodotto nel 2003 un documento contenente indicazioni circa le modalità di impiego delle tecniche di riconoscimento biometrico utilizzate per finalità di autenticazione e verifica, sollevando preoccupazioni in ordine alla tutela dei diritti e delle libertà fondamentali degli individui, che potrebbero essere lesi dal facile e non giustificato ricorso al trattamento di dati biometrici nelle procedure informatizzate di verifica e identificazione dei cittadini⁵.

4. Il governo elettronico: quale sicurezza per i cittadini?

Le politiche di governo elettronico sono diventate uno dei punti strategici del piano europeo per la Società dell'informazione, che ha individuato nelle moderne tecnologie uno strumento fondamentale per lo sviluppo socio-economico e, con l'evoluzione dei nuovi media, un mezzo efficiente per favorire il buon governo e una nuova forma di democrazia (Amoretti 2006, Zuccarini 2007).

Oggi, la nozione di governo elettronico include una serie di politiche connesse all'introduzione dell'ICTs (soluzioni organizzative, tecnologiche, informatiche e infrastrutturali) che consentono la raccolta, la conservazione, il trattamento, la trasmissione, l'interscambio e la sicurezza di informazioni e dati digitali; in questo senso si può parlare, laddove essa si realizza, di una organica politica di governo elettronico in cui non è più sufficiente creare infrastrutture e reti di interconnessione, né è sufficiente ampliare l'accesso alle informazioni con la creazione di servizi informativi aperti se, poi, non si è in grado di garantire che tutte le informazioni detenute dalle amministrazioni siano raccolte e conservate in formato elettronico e messe a disposizione avvalendosi delle ICTs, e se le amministrazioni non sono in

⁵ In argomento si consulti il *Documento di lavoro sulla biometria*. Gruppo di lavoro per la tutela dei dati personali presieduto da S. Rodotà – Istituto a norma dell'art. 29 della Direttiva 95/46/CE. Bruxelles, 13 giugno 2003.

grado di assicurare la necessaria qualità delle informazioni raccolte e la loro necessaria sicurezza (Merloni 2005, 5-12).

I punti centrali delle politiche di governo elettronico di ultima generazione riguardano, dunque, la delicata questione dell'interoperabilità, della valorizzazione del patrimonio informativo pubblico e della valutazione dell'impatto organizzativo nella gestione informatica delle informazioni. Ogni processo, viene analizzato e valutato a partire dall'organizzazione del sistema documentale informatico che, in termini di sicurezza, rappresenta uno strumento giuridico fondamentale per la riduzione ed il controllo del rischio; è nell'osmosi fra concetti tecnici e istituti giuridici, come nel caso dell'adozione del documento informatico e della firma digitale, che si realizza più propriamente la funzione regolativa della politica del governo elettronico (De Rosa 2007, 97).

Sul piano giurisprudenziale la definizione di documento informatico assume rilevanza quando la rappresentazione di fatti o pensieri elaborati con un linguaggio informatico⁶ diviene oggetto di attacchi e frodi da parte dei *computer crimes*, categoria che attiene ai reati contro i sistemi informatici e sui programmi informatici.

La prima definizione formale di documento informatico risale al 1993 ed è elaborata da una norma penale, la Legge n. 547/1993 che introduce l'art. 491 bis c.p. con cui si precisa che *“per documento informatico si intende qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli”* e si evince la rilevanza attribuita all'aspetto formale rappresentato dal *“supporto”* (valutando in secondo piano i dati che quest'ultimo contiene). L'esigenza di regolamentare l'ambito con una norma penale risiede nel fatto che il sistema penale risponde, per obbligo costituzionale, al principio di stretta legalità e di tipicità e mal si presta all'estensione e all'utilizzo di analogie per disciplinare *nuovi beni e nuove forme di aggressione*. Ciò ha portato il legislatore a produrre strumenti di tutela immediata contro la crescente serie di aggressioni e falsificazioni documentali (Petroni 1995).

A distanza di pochi anni si aggiunge una definizione giuridica esaustiva e completa di documento informatico anche sul piano civile (Martino 1998) con il D.P.R. n. 513/199, secondo cui *“il documento informatico costituisce la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti”*. Con la stessa norma il legislatore introduce, anticipando gli altri paesi UE, la firma digitale quale strumento idoneo a validare il documento informatico e adotta, quale presupposto tecnologico, il sistema della crittografia asimmetrica basata su una coppia di chiavi, una privata (e quindi segreta) ed una pubblica (visibile a chiunque).

⁶ Tecnicamente, per documento informatico si intende un documento espresso in linguaggio binario i cui dati sono elaborati mediante l'utilizzo di strumenti informatici e contenuti come impulsi elettronici nella memoria di un elaboratore o di un altro tipo di supporto informatico. Si tratta di dati non direttamente percepibili dall'insieme delle funzioni organiche sensoriali, ma comunque idonei ad essere riprodotti in forma intelligibile e visibile.

Con l'emanazione del D. Lgs n. 82/2005, Codice Amministrazione Digitale, si rafforzano gli elementi che caratterizzano il documento informatico, tra cui: a) la rappresentazione informatica e la rilevanza giuridica degli atti, dei dati e dei fatti; b) l'importanza dei requisiti tecnici che devono essere rispettati per caratterizzare il documento informatico come documento scritto e con efficacia probatoria. Si rafforzano anche i requisiti fondamentali: 1) l'integrità del documento formato (ma anche archiviato e conservato); 2) l'immutabilità nel tempo del contenuto del documento; 3) l'esatto riferimento ad un soggetto determinato quale autore del documento. Il documento informatico, sottoscritto con firma elettronica (o digitale), soddisfa il requisito della forma scritta, se il formato utilizzato per la formazione del documento garantisce la "non modificabilità".

Il processo di revisione del sistema documentale trova sbocco in progetti che fondono insieme il principio della sicurezza con l'opportunità di erogare migliori servizi al cittadino, quali il rilascio della *Carta di Identità Elettronica*, del *Passaporto Elettronico* e del *Permesso di Soggiorno Elettronico*, che prevedono l'uso della biometria per il riconoscimento certo delle persone, ma anche il progetto di rilascio della *Carta Multiservizi della Difesa* che nasce con lo scopo di ottemperare ad esigenze istituzionali e organizzative, per le quali la centralità della sicurezza è indiscutibile, soprattutto in considerazione delle criticità legate all'impiego di contingenti militari e alla necessità di dover proteggere l'enorme mole di dati contenuti nei vari sistemi informativi.

I progetti posti in essere, evidenziano, tuttavia, la prevalenza di un approccio di tipo tecnocentrico, in cui la scelta della tecnologia diventa vincolante nel processo di riorganizzazione e ammodernamento degli apparati pubblici, con una attenzione ai cittadini per lo più connessa all'esigenza di garantire la sicurezza dei servizi digitali ed incrementare il livello di fiducia nell'utilizzo degli stessi. Questo è quanto emerge dalle stesse *Linee Guida per l'impiego delle tecnologie biometriche* (2004) del Centro nazionale per la pubblica amministrazione (CNIPA), nonostante lo sforzo di prevedere l'uso combinato di più tecnologie per l'impiego di dati biometrici (con certificati di autenticazione e *smart card*) al fine di associare la sicurezza offerta da un supporto elettronico alla certezza dell'identità del possessore ed infine al rispetto dei requisiti previsti in tema di privacy.

Governo elettronico e amministrazione digitale⁷, così come delineati a partire dall'emanazione del D.lgs n. 39/1993 e fino all'entrata in vigore del D.lgs n. 82/2005 (Codice dell'Amministrazione Digitale) rappresentano un nuovo paradigma al quale le amministrazioni pubbliche dovranno fare riferimento in ordine alla strategia politica da adottare, e evidenziano la necessità di riportare l'attenzione sui processi di riorganizzazione delle strutture e delle funzioni interne (Limone 2008) in un moderno rapporto

⁷ Sull'argomento si veda R. De Rosa, *Definizioni di Governo elettronico e Amministrazione elettronica* consultabili sul sito www.federica.unina.it, 04/09/2009.

stato/cittadino, esclusivamente regolato secondo i principi che antepongono le condizioni organizzative a quelle tecnologiche, come prerequisito di queste ultime.

Si condivide in questo senso la prospettiva secondo cui «il governo elettronico non risponde alle leggi informatiche ma a quelle della politica» (De Rosa 2007, 8), oltre alla necessità di superare una ambivalenza teorica che rischia di porre il governo elettronico in una zona d'ombra a metà fra un semplice processo di digitalizzazione della Pubblica amministrazione e una straordinaria occasione per promuovere la trasparenza, l'accesso, l'informazione e la partecipazione (Calise, De Rosa 2003, 279), alcuni dei più importanti principi della democrazia e della cittadinanza in rete.

Riferimenti bibliografici

- Acuña E.R. (2002) *Habeas data costituzionale: nuova garanzia giurisdizionale del diritto pubblico latinoamericano* in “Diritto Pubblico comparato ed Europeo”, n. 4, pp. 1921-1945.
- Alexy R. (2002) *A theory of constitutional right*, Oxford University Press, New York.
- Amoretti (2006) *La rivoluzione digitale e i processi di costituzionalizzazione europei. L'e-democracy tra ideologia e pratiche istituzionali*, in “Comunicazione Politica”, n. 1, pp. 49-74.
- Barcellona P. (2005) *Il suicidio dell'Europa: dalla coscienza infelice all'edonismo cognitivo*, Edizioni Dedalo, Bari.
- Bell D. (1974) *The coming of postindustrial society: a venture in social forecasting*, Penguin, Harmondsworth.
- Bin R., Pitruzzella G. (2001) *Diritto Costituzionale*, Giappichelli, Torino.
- Bobbio N. (1990) *L'età dei diritti*, Einaudi, Torino.
- Calise M., De Rosa R. (2003) *Il governo elettronico: visioni, primi risultati e un'agenda di ricerca*, in “Rivista Italiana di Scienza Politica”, vol. 33, n. 2, pp. 257-283.
- Castells M. (2000) *The Information Age: Economy, Society, and Culture*, Blackwell, Oxford.
- Id. (2002) *La nascita della società in rete*, trad. it., EGEA, Milano.
- Crescentini A. (2007) *Elogio della sicurezza: aspetti multidisciplinari tra scienza e pratica*, Vita e Pensiero, Milano.
- De Rosa R. (2007) *Il cuore del governo elettronico*, in “POLIS”, XXI, n. 1, pp. 95-115.
- Downey J.W., McGuigan J. (1999) *Technocities*, SAGE, London.
- Foucault M. (2005) *Sicurezza, Territorio, Popolazione*, Feltrinelli, Milano.
- Id. (2005) *Nascita della Biopolitica*, Feltrinelli, Milano.
- Frosini V. (1991) *Contributi ad un diritto dell'informazione*, Liguori, Napoli.
- Gamaleri G. (1998) *Le ambivalenze d'oggi*, in J. Jacobelli (a cura di) *La realtà del virtuale*, Laterza, Roma-Bari.
- Goodman, J.W. (2006) *Telecommunications policy-making in the european union*, E.E. Publishing, Cheltenham.
- Limone D. A. (1999) *Elementi di diritto dell'informatica*, Editrice Salentina, Lecce.
- Id. (2008) *Rivoluzioni organizzative: la teoria dei paradigmi di Thomas Kuhn*, in “eGov - Cultura e tecnologie per l'innovazione”, n. 1/2, pp. 17-19.
- Lyon, D. (1991) *La società dell'informazione*, Il Mulino, Bologna.
- Id. (2002) *La società sorvegliata. Tecnologie di controllo della vita quotidiana*, Feltrinelli, Milano.
- Luhmann N., De Giorgi R. (1994) *Teoria della società*, FrancoAngeli, Milano.
- Luhmann N. (2002) *I diritti fondamentali come istituzione*, Edizioni Dedalo, Bari.
- Martino A. A. (1998) *Nuovo regime giuridico del documento informatico*, FrancoAngeli, Milano.
- McLuhan M. (1999) *Gli strumenti del comunicare*, Il Saggiatore, Milano.
- Merloni F. (2005) *Introduzione all'e-government*, Giappichelli, Torino.
- Padovani G., Nesti G. (2003) *La dimensione regionale nelle politiche dell'UE per la Società dell'informazione*, in Messina P. (a cura di) *Sistemi locali e spazio pubblico europeo*, Carocci, Roma, pp. 207-227.
- Paye J. (2007) *Global war on liberty*, Telos, New York.
- Peces-Barba G. (1993) *Teoria dei diritti fondamentali*, Giuffrè, Milano.
- Petrone M. (1995) *Le recenti modifiche del codice penale in materia di documento informatico*, in “Diritto dell'Informazione e dell'Informatica”, n. 2, pp. 259-276.
- Pickering A. (2001) *La scienza come pratica e come cultura*, Edizioni di Comunità, Torino.
- Pinch, T., Bijker, W. e Hughes, T. (1987) *The Social Construction of Technological Systems*, MA MIT Press, Cambridge.

- Powell, W.W. (1990) *Neither market nor hierarchy: network forms of organization*, in Cummings, L.L. e Staw, B.M. (eds.), *Research in Organizational Behavior*. Greenwich, CT: JAY Press.
- Preite G. (2008) *Il riconoscimento biometrico. Sicurezza versus privacy*, UNI Service, Trento.
- Ragnedda M. (2006) *Eclissi o tramonto del pensiero critico. Il ruolo dei mass media nella società post-moderna*, Aracne, Roma.
- Rodotà S. (2004) *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Laterza, Roma-Bari.
- Id. (2005) *Intervista su privacy e libertà*, Laterza, Roma-Bari.
- Id. (2006) *La vita e le regole: tra diritto e non diritto*, Feltrinelli, Milano.
- Sabattini G. (2003) *Globalizzazione e governo delle relazioni tra i popoli*, FrancoAngeli, Milano.
- Servaes, J. (2003) *The european information society*, Bristol, Intellect.
- Stonier T. (1983) *The wealth of information: a profile of the post-industrial economy*, Thames Methuen, London.
- Touraine A. (1970) *La società post-industriale*, Il Mulino, Bologna.
- Van Dijk J. (2002), *Sociologia dei nuovi media*, Il Mulino, Bologna.
- Zuccarini M. (2007) *Dieci anni di governo elettronico in Italia: destra e sinistra a confronto*, in "POLIS", XXI, n. 1, pp. 9-30.