Gianfranco Gabriele

Parlamentarismo ed evoluzione tecnologica: un nuovo modello di partecipazione e di rappresentanza

1 - Premessa; 2 - Parlamentarismo ed evoluzione tecnologica; 3 - Un nuovo modello di partecipazione e di rappresentanza; 4 - La tecnologia informatica a supporto dei nuovi modelli di partecipazione e rappresentanza; 4.1 - La crittografia a chiavi pubbliche, la firma digitale, l'autorità di certificazione; 5 - Una procedura per l'attribuzione elettronica del voto segreto; 6 - Conclusione.

1 - *Premessa*

L'abbinamento della parola «parlamentarismo» e dell'espressione «evoluzione tecnologica» può apparire come un accostamento poco usuale.

In effetti, «parlamentarismo» viene associato immediatamente, nell'immaginario collettivo, alla migliore tradizione della cultura giuridico-umanistica, alla quale però, fatte le dovute eccezioni, è completamente estranea qualsiasi contaminazione tecnologica. Da questo punto di vista, anzi, la tecnologia viene spesso considerata come lo studio di arti banali, adatte ai soli tecnici, categoria, quest'ultima, ritenuta composta da professionalità piuttosto indistinte ad eccezione dei meccanici, degli elettricisti e degli idraulici.

La tecnologia naturalmente più versata al parlamentarismo, in realtà, è quella informatica e delle comunicazioni, oggetto di un tumultuoso sviluppo e di un numero pressoché illimitato di applicazioni in ogni campo delle attività umane. Il quadro normativo, d'altra parte, con il riconoscimento della legittimità a tutti gli effetti di legge del documento e della firma elettronica ([1]), si è impreziosito di una componente dagli enormi risvolti sul piano dell'efficienza e dell'efficacia delle comunicazioni tra cittadino ed istituzioni, ed ha accentuato il ruolo centrale dell'informatica e delle comunicazioni nella riorganizzazione dei processi distintivi della pubblica amministrazione.

Il parlamentarismo, per parte sua, è realmente posto sotto pressione ([2]) dal moltiplicarsi dei centri di decisione che trascendono il quadro

parlamentare, da una crisi di rappresentatività che favorisce l'allontanamento dei cittadini dalle istituzioni, da una maggiore velocità e capacità di risposta dei gruppi di interesse al modificarsi del mercato, della situazione sociale ed internazionale.

Il presente lavoro, partendo da quest'insieme di considerazioni, si propone soprattutto di evidenziare, attraverso la rappresentazione di un nuovo modello di partecipazione e di rappresentanza, le potenzialità insite nelle attuali tecnologie. Queste ultime, se usate correttamente, dal momento che lasciano la mente libera di ipotizzare, progettare e realizzare soluzioni senza i condizionamenti ed i vincoli precedenti l'attuale fase dell'informatica, possono rappresentare un aiuto fondamentale nella definizione di nuovi assetti istituzionali.

Il modello esposto propone di coniugare, attraverso la tecnologia informatica ed all'interno dello stesso sistema democratico, sia istanze di partecipazione diretta alle deliberazioni, sia istanze di rappresentanza sulla base di specifiche deleghe per grandi aree tematiche. Un ampliamento del modello potrebbe definire le caratteristiche ed i rapporti con le altre istituzioni, quali il Presidente della Repubblica, il Governo, la Corte costituzionale, la Magistratura.

Il lavoro si svolge su quattro capitoli ed una conclusione. Nel capitolo *Parlamentarismo ed evoluzione tecnologica*, viene concisamente illustrata la storia dei rapporti che hanno legato l'evoluzione informatica ed il Parlamento, passando in rapida rassegna i progetti che si vanno realizzando, finalmente rivolti ai processi di formazione della legge, ma ponendosi anche il quesito cruciale: tutto questo è sufficiente?

Il capitolo successivo, sottintendendo una risposta negativa al precedente quesito, propone *Un nuovo modello di partecipazione e di rappresentanza*, illustrandone con un certo dettaglio il funzionamento, fondato sull'informatica e le comunicazioni.

Il capitolo *La tecnologia informatica a supporto dei nuovi modelli di partecipazione e di rappresentanza*, si sofferma su aspetti più tecnici, la cui comprensione è però auspicabile perché venga fugata ogni incertezza nei riguardi della sicurezza, del rispetto della privacy e della mancata materializzazione, almeno per questa via, del «grande fratello». Inoltre, per chi non ha familiarità con i meccanismi delle chiavi pubbliche e private, rappresenta un'utile introduzione al capitolo successivo.

Infatti, nel capitolo *Una procedura per l'attribuzione elettronica del voto segreto*, si presenta una procedura che consente di esprimere in modo anonimo il proprio voto, alla stregua di quanto avviene nelle attuali operazioni di voto presso i seggi elettorali. Dal confronto delle due

procedure, manuale ed informatica, dovrebbe conseguire una sufficiente confidenza nella praticabilità della soluzione.

Infine, nella *Conclusione*, ricapitolati alcuni aspetti chiave, si ipotizza una possibile via di sperimentazione concreta del modello proposto o di analoghe soluzioni.

2 - *Parlamentarismo ed evoluzione tecnologica*

Tutto evolve con grande velocità. Cambiano le abitudini e i ritmi del vivere insieme; le modalità con cui si produce, si comunica, si commercia. In ogni settore ci si attrezza sui due versanti della globalizzazione e del riconoscimento, della soddisfazione, delle specificità. Il motore propulsivo fondamentale che spinge e costringe al cambiamento è rappresentato dal binomio competizione di mercato ed evoluzione tecnologica. Una evoluzione, quest'ultima, che permea ogni attività, che spinge fuori mercato chiunque non si affretti ad adottarla, a prevederne ed anticiparne gli effetti. Da ancella di un potere guerriero, a cui offriva servigi per ricevere in cambio promozione e soddisfazione, la tecnologia — in tutte le svariate forme della sua applicazione: dalla biologia alla medicina, dall'informatica alla comunicazione, dalla fabbrica all'agricoltura — è divenuta la vera grande signora, la più temuta e corteggiata, dello sviluppo e della competizione di mercato.

Ai fini di questo lavoro, per la natura dell'argomento trattato, l'evoluzione tecnologica più pertinente da considerarsi è quella intervenuta nel mondo dell'informatica e delle comunicazioni. Un'evoluzione tumultuosa, che nella prima fase ha cambiato le modalità di produzione attraverso l'automazione delle attività manuali e ripetitive, tanto nel mondo della fabbrica che del lavoro d'ufficio. Appartengono a questa prima generazione tanto le fabbriche robottizzate per il conseguimento della flessibilità di produzione che le prime applicazioni informatiche degli stipendi, della contabilità, della gestione di voluminosi archivi clienti e fornitori, dell'inventario, degli ordini e della fatturazione. Concettualmente, corrisponde alla stessa fase l'introduzione negli uffici dei primi sistemi di video scrittura progettati per supportare il lavoro segretariale. Anche la costruzione di grandi banche dati bibliografiche e normative, in questa fase, è pensata più nell'ottica dell'informatizzazione degli archivi che della fruibilità e del supporto conoscitivo per generici utenti.

Siamo a cavallo tra la fine degli anni '60 e l'inizio degli anni '70 e la Camera dei deputati, ma altrettanto fa il Senato, è pronta a cogliere i vantaggi derivanti dall'adozione della tecnologia informatica. Anzi, si dota di personale informatico, vara progetti all'avanguardia nell'area delle banche dati legislative e costruisce un sistema informatico amministrativo adeguato ai tempi. D'altra parte, i benefici derivanti dall'adozione di questa prima informatizzazione sono facilmente comprensibili a chiunque. Si tratta essenzialmente di ridurre i costi tangibili, di risparmiare tempi facilmente misurabili e, soprattutto, di modificare soltanto il lavoro di tipo esecutivo. I funzionari, la dirigenza e tutto il personale politico non sono minimamente toccati, nè interessati, dal cambiamento.

La dimostrazione di ciò è nelle cose. Comincia, esaurito lo slancio di questa prima fase, il divario tra il nuovo ruolo che l'informatica va assumendo nelle organizzazioni complesse e la sua percezione, ancor prima della sua applicazione, all'interno del Parlamento. L'informatica, in quella che per semplicità potremmo chiamare la sua seconda fase, diventa tecnologia di riorganizzazione, di direzione, controllo e pianificazione, di supporto alle decisioni attraverso l'analisi e la modellizzazione della conoscenza, anche destrutturata, rilevata dai processi di lavoro e trasferita alla direzione. Di questo passaggio, che avrebbe dovuto quantomeno coinvolgere rappresentanza politica, dirigenza e personale informatico, non vi è memoria; non vi è stata, per lungo tempo, nessuna riflessione foriera di risultati.

Negli anni '90, la distanza nella percezione del ruolo dell'informatica cresce ancora. L'informatica ha ormai assunto, nella sua terza fase, il ruolo di tecnologia a supporto delle transazioni, trova motivazioni nell'affermarsi come tecnologia indispensabile al *core business* delle organizzazioni, diviene risorsa preziosa per il conseguimento di vantaggi competitivi. Il Parlamento, da questo punto di vista, è ancora assente. Non pare avvertire l'esigenza di sviluppare una nuova cultura della tecnologia che finisca per permearlo, di dotarsi di un sistema informativo efficiente per l'assunzione delle decisioni, la valutazione degli impatti, in definitiva, di ripensare fino in fondo il ruolo dell'informatica per porlo al centro del proprio *core business*, che è poi quello di fare buone leggi.

Probabilmente è inutile rincorrere responsabilità, ma l'intreccio tra la disattenzione politica, l'incultura e la diffidenza tecnologica di una dirigenza amministrativa tutta orientata al mondo giuridico ed umanistico, l'incapacità o l'impossibilità dei responsabili informatici di trovare credito ed ascolto, ha rappresentato una miscela che per lungo tempo ha paralizzato ogni serio sviluppo dell'informatica parlamentare.

Soltanto di recente, negli ultimi anni, la nuova dirigenza politica ed amministrativa ha cominciato, lentamente, a percepire il divario che si era aperto tra le potenzialità dell'informatica, espresse con successo in ogni settore delle attività umane e delle organizzazioni, e il ruolo marginale assunto dall'informatica parlamentare. All'interno del Parlamento si è quindi cominciato ad operare freneticamente nel tentativo di recuperare i molti, troppi, anni di indifferenza.

Ai grandi progetti a valenza più strettamente tecnica, rivolti essenzialmente alla rifondazione delle infrastrutture informatiche di elaborazione, comunicazione ed assistenza, e che rappresentano il presupposto alle realizzazioni applicative, si comincia ad affiancare, finalmente, una informatizzazione che è parte integrale, non giustapposta o descrittiva, del processo di lavoro conoscitivo e decisionale. Ciò coinvolge tanto le attività legislative e di sindacato, quanto quelle di auto-amministrazione del Parlamento.

Si intraprendono sforzi significativi nella promozione degli strumenti informatici ad uso personale per i parlamentari; risponde a questa istanza la dotazione effettuata di personal computer portatili, di pacchetti software di produttività individuale e di formazione, la definizione di un sistema di messaggistica con l'attivazione di caselle di posta elettronica individuali.

Un progetto già di grande visibilità è quello che trasferisce parte della comunicazione istituzionale verso i cittadini e l'accesso alle banche dati legislative e di documentazione su Internet ([3]). Sono in fase di avvio progetti per consentire forme di telelavoro per i deputati che, in tal modo, potranno più facilmente conciliare gli impegni presso il Parlamento con la necessità di rapportarsi al territorio, in particolare quello dei collegi.

È prevista la realizzazione di progetti, per alcuni dei quali la fase di prima istruzione è sostanzialmente terminata, nelle aree del *drafting* legislativo, della fattibilità e della simulazione degli effetti della legge, dell'osservatorio sulla legislazione.

Tale appassionato riprogettare e ricostruire un'informatica parlamentare adeguata nel ruolo e nei compiti all'imperio dei tempi e alle esigenze fondamentali dell'Istituto si confronta continuamente da una parte con antiche e radicate resistenze, con cupe previsioni di insuccesso, e dall'altra con l'insoddisfazione ed il disagio di chi già vorrebbe colmato il divario accumulato negli anni.

Non vi è dubbio, comunque, che se, nonostante tutto, il processo di cambiamento verrà sostenuto ed alimentato dai vertici politici ed ammi-

nistrativi almeno oltre il punto di non ritorno, in tempi brevi ma congrui rispetto alla serietà dell'impegno, con soluzioni di maggior o minor gradimento, l'evoluzione tecnologica e culturale necessaria per portare il Parlamento a fruire di servizi informativi paragonabili a quelli di strutture complesse e competitive sarà compiuto. D'altra parte, il conseguimento di questo obiettivo non è un capriccio: è assolutamente necessario, se si vuole che il Parlamento conservi un'autonoma capacità di indagine, ricognizione, comprensione, elaborazione e decisione, sia dal Governo che dai gruppi di interesse.

Ma tutto questo è sufficiente? può bastare, o il Parlamento deve esercitare una funzione progettuale di ampio respiro che ponga in discussione anche il suo attuale assetto, il suo modo d'operare e persino le sue stesse finalità, disegnando scenari in cui la tecnologia diviene una componente strutturale delle risposte da elaborare per soddisfare le nuove istanze di partecipazione e di rappresentanza democratica?

Nella storia dell'evoluzione informatica, così come sin qui interpretata, siamo ormai arrivati alla quarta fase: quella in cui l'informatica assume il ruolo di integratore, ad alto valore aggiunto, delle diverse matrici tecnologiche sia della comunicazione — la televisione, il telefono, il fax, la trasmissione dati — sia della gestione delle informazioni — dati strutturati, testi, disegni, immagini, suoni, video — , in una rappresentazione ipermediale della conoscenza. L'informatica diviene pervasiva, perde molti dei connotati di una tecnologia a se stante per diluirsi nei mille rivoli delle piccole comodità quotidiane, componente essenziale per concludere affari, per scambiare informazioni ed esperienze tra genti diverse e lontanissime, per il divertimento ed il tempo libero, per la costituzione di comunità virtuali.

L'espressione più evidente di questa evoluzione è certamente rappresentata dall'entusiasmante successo che va ottenendo Internet in tutto il mondo. Soffermandosi, in particolare, sulla realtà italiana, studi condotti soprattutto (e ovviamente) sulle caratteristiche e possibilità del commercio elettronico raffigurano una situazione dinamica in forte espansione che può già contare su un numero di utilizzatori estremamente significativo. A maggio del 1998, circa 2.600.000 italiani adulti hanno dichiarato di aver utilizzato Internet nel mese precedente ([4]). Il dato è particolarmente significativo non solo in assoluto, ma soprattutto se comparato alla stima effettuata nello stesso periodo dell'anno precedente, che posizionava il numero di utenti in 1.500.000. Il fenomeno dimostra un'eccezionale dinamica, se è vero che da gennaio a maggio si sono contati 682.000 nuovi utenti e che si stima, nello stesso periodo, in

circa 550.000 il numero degli italiani che hanno sottoscritto contratti per collegarsi ad Internet da casa. Dati piacevolmente sorprendenti anche sull'utilizzazione che, nonostante la bassa velocità di navigazione penalizzi le aspettative e la soddisfazione d'impiego, è stata misurata in oltre un milione e mezzo di utenti italiani che si collegano ad Internet almeno una volta alla settimana, in circa 770.000 che la utilizzano giornalmente ed è stato valutato in 850.000 il numero degli utenti che, anche occasionalmente, consultano le *news online*.

Questi dati sono significativi per rilevare una tendenza che non può assolutamente liquidarsi come un fenomeno passeggero o di moda. In realtà, è facile prevedere che il circuito virtuoso della «proliferazione dei servizi disponibili in Internet — sempre maggiore utenza — ulteriore incremento dell'offerta dei servizi» venga letteralmente esaltato dalla disponibilità di nuove infrastrutture di rete (prevedibilmente con grande ricorso ai satelliti) e di apparati (quali telefoni e televisioni con browser Internet integrati) che sempre meno richiameranno le difficoltà di impiego e gestione degli attuali computer e sempre più saranno assimilati ad indispensabili e semplici oggetti d'uso quotidiano. Questa riflessione non è una esaltazione di Internet fine a se stessa; infatti, la capillare diffusione della rete rappresenta un elemento fondamentale nello svolgimento del ragionamento che si sta conducendo e che proietta l'impiego di Internet, per una volta, non verso il commercio elettronico, ma verso la partecipazione democratica alla vita politica del paese.

Al progresso compiuto dalla tecnologia informatica, si è affiancato, in Italia, un quadro normativo di grande rilievo relativo al documento ed alla firma elettronica. La legge 15 marzo 1997, n. 59 (Delega al governo per il conferimento di funzioni e compiti alle Regioni ed enti locali, per la riforma della pubblica amministrazione e per la semplificazione amministrativa), in particolare all'articolo 15, comma 2, riconosce che «Gli atti, dati e documenti formati dalla pubblica amministrazione e dai privati con strumenti informatici, sono validi e rilevanti a tutti gli effetti di legge». Tale disposto, insieme al relativo regolamento contenente i criteri e le modalità di applicazione e alle regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici ([5]), costituisce anch'esso un passaggio essenziale per la comunicazione via rete dei cittadini tra loro e con le istituzioni. Un'ulteriore sinergia potrebbe realizzarsi con l'approvazione del riconoscimento della validità giuridica del documento d'identità personale nel formato elettronico. In questo caso, potrebbe essere quest'ultimo il supporto per la gestione delle chiavi pri-

vate e pubbliche per la firma elettronica e la cifratura/decifratura dei documenti come si tornerà a dire più compiutamente nel seguito.

Così tratteggiati i temi dell'evoluzione delle tecnologie dell'informazione ed il quadro normativo di maggior interesse ai fini di questo lavoro, riprendendo i quesiti poc'anzi formulati, la questione è: ma il parlamentarismo è esente dall'influenza dei tempi, dalla complessità della società attuale, dal moltiplicarsi dei centri di decisione e di produzione di regole?

Sempre più frequentemente istituti fondamentali della rappresentanza quali, ad esempio, l'assenza di vincolo di mandato e il ruolo dei partiti, vengono posti sotto l'accusa di inadeguatezza, di non rispondenza, dopo il ruolo storico giocato, alle esigenze dei tempi. Anche recentemente, se ne è avuta una significativa dimostrazione indiretta. Senza assolutamente voler entrare nel merito della questione specifica, in occasione della crisi del Governo Prodi e della formazione del Governo D'Alema, in presenza di accuse pesanti di tradimento rivolte ai parlamentari che hanno cambiato schieramento politico, non è sostanzialmente mai stato richiamato da nessuno, «illanguidito sino a sembrare ormai anacronistico» ([6]), l'articolo 67 della Costituzione che attraverso la negazione del vincolo di mandato intende tutelare l'interesse generale su quello particolare ([7]). D'altra parte, politologi come Bobbio, al proposito affermano: «Mai norma costituzionale è stata più violata del divieto di mandato imperativo. Mai principio è stato più disatteso di quello della rappresentanza politica» e con esplicito riferimento ai partiti: «Nel parlamento? Ma che cosa rappresenta la disciplina di partito se non una aperta violazione del divieto di mandato imperativo?» ([8]). Considerazione che subito si salda sul ruolo della difesa di interessi particolari assunto dai partiti ([9]), una volta esaurita la spinta iniziale in cui «hanno favorito la crescita del paese e della stessa democrazia» ([10]), per arrivare alla conclusione che «i partiti politici ... sono diventati organizzazioni come tante altre» ([11]).

Inoltre, «molte delle istanze strategiche di dibattito, negoziato, soluzione dei conflitti e regolazione trascendono il quadro parlamentare. I soggetti principali sono gruppi, organizzazioni e reti all'interno della società civile. ... In sintesi, le democrazie nazionali costituite dai singoli cittadini e dai loro rappresentanti parlamentari tendono ad essere oltrepassate da una democrazia diretta di fatto, fatta di interessi organizzati, lobby e movimenti direttamente impegnati nelle questioni di proprio interesse» ([12]). In definitiva sembra diffondersi la consapevolezza, per usare ancora le efficaci espressioni di Burns, che «senza una effettiva

ridefinizione del ruolo e della funzione della democrazia rappresentativa, la profonda incapacità e marginalizzazione di essa probabilmente non solo continueranno, ma contribuiranno a una perdita di fiducia e di sostegno verso le istituzioni democratiche. Diventerà sempre più difficile mantenere l'immagine pubblica della centralità della democrazia parlamentare di fronte ai crescenti deficit democratici e all'ampio divario tra responsabilità presunte e reali capacità di governo» ([13]).

Si può affermare che pur con sfumature ed importanti distinguo, sull'analisi della crisi del parlamentarismo, si assiste ad una sostanziale convergenza d'opinioni. Sono, ovviamente, le soluzioni alla crisi che ognuno propone a differenziarsi anche sostanzialmente.

Nello spirito della trattazione sin qui condotta, e cioè della centralità della tecnologia nella riprogettazione dei processi, in particolare quelli di servizio, si è avanzata un'ipotesi che, se pure non nuova nel riferimento alla tecnologia informatica ([14]), è parsa rispondente sia al nuovo ruolo assunto dall'informatica che all'esigenza di coniugare all'interno dello stesso sistema democratico, a piacimento del cittadino, sia istanze di partecipazione diretta alle decisioni che istanze di rappresentanza sulla base di specifiche deleghe.

Poiché i capitoli successivi sono dedicati all'esposizione di questo nuovo modello di partecipazione e rappresentanza basata sulla componente informatica, in questo ci si sofferma a sintetizzare l'insieme di giudizi e pregiudizi, osservazioni e perplessità sollevate da soluzioni qualificate come di teledemocrazia. Un po' slealmente, in quanto ci si riferisce ad articoli pubblicati per la prima volta nel 1984, ma per guadagnare in espressività e sintesi, si riportano di seguito due brani emblematici.

«L'ipotesi che la futura computer-crazia, com'è stata chiamata, consenta l'esercizio della democrazia diretta, cioè dia a ogni cittadino la possibilità di trasmettere il proprio voto a un cervello elettronico, è puerile. A giudicare dalle leggi che vengono emanate ogni anno in Italia il buon cittadino dovrebbe essere chiamato a esprimere il proprio voto almeno una volta al giorno. L'eccesso di partecipazione, che produce l'effetto che Dahrendorf ha chiamato, deprecandolo, del cittadino totale, può avere per effetto la sazietà della politica e l'aumento dell'apatia elettorale. Il prezzo che si deve pagare per l'impegno di pochi è spesso l'indifferenza di molti. Nulla rischia di uccidere la democrazia più che l'eccesso di democrazia» ([15]).

«Se ho manifestato qualche dubbio che la computer-crazia possa giovare alla democrazia governata, non ho alcun dubbio sul servizio che può

rendere alla democrazia governante. L'ideale del potente è sempre stato quello di vedere ogni gesto e di ascoltare ogni parola dei suoi soggetti (possibilmente senza essere visto né ascoltato): questo ideale oggi è raggiungibile. Nessun despota dell'antichità, nessun monarca assoluto dell'età moderna, pur circondato da mille spie, è mai riuscito ad avere sui suoi sudditi tutte quelle informazioni che il più democratico dei governi può attingere dall'uso di cervelli elettronici. La vecchia domanda che percorre tutta la storia del pensiero politico: «Chi custodisce i custodi?» oggi si può ripetere con quest'altra formula «Chi controlla i controllori?». Se non si riuscirà a trovare una risposta adeguata a questa domanda, la democrazia, come avvento del governo visibile, è perduta» ([16]).

In un altro articolo, però, lo stesso Bobbio — con lungimiranza, ma forse anch'egli sottovalutando la rapidità dell'evoluzione tecnologica — affermava: «Nessuno può immaginare uno Stato che possa essere governato attraverso il continuo appello al popolo: tenendo conto delle leggi che vengono emanate nel nostro paese all'incirca ogni anno si dovrebbe prevedere in media una chiamata al giorno. Salvo nella ipotesi per ora fantascientifica che ogni cittadino possa trasmettere il proprio voto a un cervello elettronico standosene comodamente a casa e schiacciando un bottone» ([17])

Come si vedrà nel prossimo capitolo, la flessibilità e le possibilità offerte dalla tecnologia informatica sono tali che non obbligano affatto l'adozione di modelli rigidi: tra la delega totale, e senza vincolo di mandato da una parte, alla partecipazione diretta dall'altra, è possibile gestire un ampio spettro di posizioni intermedie tra loro compatibili. In questa ottica, non si manifesta un «eccesso di democrazia» ma piuttosto la libera valutazione della modalità, soggettivamente ritenuta preferibile, con cui partecipare alle scelte democratiche. Il convincimento di fondo è il seguente: ogni cittadino è disponibile a delegare il proprio mandato ad una persona o ad una organizzazione di cui si fida, se continua ad averne il continuo controllo (immediata possibilità di revocare la delega). E se è certamente vero, per svariati ordini di motivi, che un cittadino non possa seguire direttamente ogni provvedimento e quindi, nella maggioranza dei casi, usufruirà della possibilità di delegare, è altrettanto «democraticamente» rilevante che ogni qual volta, su provvedimenti che a suo giudizio lo toccano direttamente, nei convincimenti come negli interessi, vuole esprimersi direttamente deve avere la possibilità di farlo.

Per terminare queste considerazioni di ordine generale, l'informatica, il computer, come ogni altra tecnologia, è sostanzialmente neutrale. Che l'uomo ne abbia fatto e ne faccia un uso improprio e cattivo, che l'abbia

spesso usata ferocemente contro l'uomo stesso, non modifica il fatto che sono le modalità di impiego, le procedure utilizzate, le finalità a rendere utile o dannosa una tecnologia. Da questo punto di vista, l'impiego corretto dell'informatica può contribuire a liberare l'uomo, a rendere ogni cosa trasparente, «visibile» per l'appunto.

3 - *Un nuovo modello di partecipazione e di rappresentanza*

Le osservazioni e le riflessioni precedentemente riportate costituiscono le motivazioni per la ricerca di modelli che, utilizzando al meglio le tecnologie della comunicazione e dell'informatica, rilancino la partecipazione dei cittadini alle scelte politiche ed amministrative senza per questo ledere gli interessi generali e riqualificando, al contempo, contenuti e modi della rappresentanza politica. Nel seguito saranno tratteggiate le caratteristiche fondamentali di un modello pensato per perseguire tali obiettivi. Se il modello si presti a conseguirli, anche soltanto nel mondo virtuale della simulazione, è tutto da dimostrare a fronte di una disamina molto approfondita. In ogni caso, non è l'unico modello ipotizzabile. Serve soprattutto a dimostrare che le potenzialità insite nelle attuali tecnologie hanno il gran pregio di lasciare la mente libera di ipotizzare, progettare e realizzare soluzioni al di fuori dei condizionamenti e delle rigidità del mondo precedente le nuove frontiere dell'informatica.

Nel modello proposto si assume che ogni cittadino venga dotato dal proprio Comune di una carta d'identità costituita da un dispositivo elettronico atto a generare e gestire, tra l'altro, una coppia di chiavi private: una per la firma elettronica e l'altra per la cifratura/decifratura dei messaggi. Attraverso tale dispositivo egli risulta univocamente e con certezza identificato dalle persone e/o organizzazioni con le quali intende intrattenere rapporti ([18]), anche utilizzando Internet. Potrà collegarsi sia da casa, se possiede una stazione di collegamento (personal computer, network computer, telefono o televisione con browser integrato) munita di apposito dispositivo per la gestione della sua carta d'identità elettronica, sia da posti pubblici dotati di analoghe stazioni (tipicamente scuole che andrebbero rinforzate nella loro dotazione informatica, biblioteche, sale dei Comuni aperte al pubblico ecc.).

Il cittadino, così equipaggiato, può decidere di partecipare direttamente già alla fase di formazione di un provvedimento, intervenendo nei

vari forum o gruppi di discussione che trattano di argomenti che sente, per professione o vocazione, a lui congeniali ([19]).

È ovvio che, per fare proposte e/o emendamenti da assoggettare ad una votazione deliberativa, dovrà adoperarsi per aggregare intorno alle sue proposte, in un tempo definito, il *quorum* prestabilito. Su questo tema si tornerà in seguito.

D'altra parte, ci sono molte tematiche che il singolo cittadino sente estranee ai suoi interessi o che comunque riconosce eccessivamente specifiche, tecniche o troppo complesse. In questo caso egli può decidere o di non partecipare oppure di delegare un altro soggetto (che può essere una persona o un'organizzazione) a rappresentarlo. Tale processo di delega, alla stregua di ogni altra operazione, avviene sempre per via telematica ed in modo assolutamente dinamico. Il cittadino, attraverso Internet, ha a disposizione una particolare applicazione informatica che gli consente in modo semplice di effettuare in ogni momento la delega o di revocarla. Potrebbe, per esempio, pensare di attribuire la delega al signor Rossi per tutto il tempo della formazione del provvedimento per revocarla, in modo da intervenire direttamente o da attribuirla ad altro soggetto, quando si tratta di effettuare la deliberazione. Ciò gli è possibile — ed è questione fondamentale — perché egli ha la completa visibilità oltre che delle azioni e delle scelte operate dal delegato anche dell'iter del provvedimento, dei termini previsti per la sua approvazione e di ogni altra cosa ad esso correlata.

Il sistema informatico preposto al governo di tali informazioni (deleghe e revoche) assicura che, relativamente ad ogni tematica, ogni cittadino esprima sempre e soltanto un solo voto.

Questo meccanismo di delega sembrerebbe molto vicino al normale modo di pensare e di fare delle persone. Certamente, ognuno ha qualcuno di cui si fida (il figlio, il fratello, l'amico, il conoscente, l'associazione, il partito politico, ...) in una certa materia più di quanto non si fidi del candidato votato su un programma generale o, più spesso, generico. Inoltre, lo tranquillizzerebbe molto il pensare che in ogni momento può riappropriarsi del suo autonomo diritto di voto.

Il meccanismo di delega dovrebbe essere pensato per poter essere utilizzato in modo ricorsivo (o transitivo), nel senso che se ad un dato istante il cittadino A delega il cittadino B ed il cittadino B delega l'organizzazione C che a sua volta delega l'organizzazione D, il voto di A, per tutto il tempo di validità delle deleghe e relativamente alla tematica rispetto alla quale è stata data, è espresso da D. Ancora una volta, la completa trasparenza di ognuna di queste operazioni e l'assenza di

qualsiasi vincolo o difficoltà nel ritirare in ogni momento la delega costituiscono le basi per assicurare al cittadino che tutto sta avvenendo sotto il completo controllo e rispetto della sua volontà. Per ulteriore sicurezza, in ogni caso, è possibile prevedere che la delega consenta ad ogni cittadino di stabilire se per essa valga, o meno, la proprietà transitiva.

Le tematiche sulle quali i cittadini, nelle modalità sopra descritte, possono esprimere direttamente la loro volontà sono praticamente in numero altissimo, soprattutto se facciamo corrispondere al concetto di tematica ogni singolo provvedimento legislativo attualmente elaborato dal Parlamento e dalle assemblee regionali e comunali. Diverrebbe pertanto estremamente impegnativo per un cittadino intervenire sempre direttamente su tutto o anche soltanto gestire un meccanismo di delega puntualmente riferito ad ogni provvedimento in discussione. Fermo restando che questa possibilità deve essere comunque garantita, un meccanismo più efficiente potrebbe essere quello di suddividere l'intero scibile sul quale pronunciarsi in grandi aree tematiche, alla stregua di quanto avviene attualmente nelle due Camere con riguardo alle commissioni. In questo modo ogni cittadino può delegare qualcun altro o rispetto ad un singolo provvedimento in discussione o rispetto ad una delle grandi aree tematiche individuate.

Nel caso di conflitto nell'attribuzione della delega — perché il signor A dà una delega al signor B per un particolare provvedimento in discussione che afferisce all'area tematica 1 per la quale sempre il signor A ha delegato l'organizzazione C — prevale la delega riferita al provvedimento. In questo modo si riconosce all'organizzazione delegata per l'area tematica la possibilità di continuare ad esprimersi su ogni restante provvedimento relativo a quell'area. Non è invece possibile, e il sistema automaticamente non lo consentirebbe, attribuire contemporaneamente la delega su uno stesso provvedimento o su una stessa area tematica a due diversi soggetti.

Un caso ancora diverso riguarda quei provvedimenti che sono a cavallo o sulla frontiera di due distinte aree tematiche e che pertanto, nell'approvazione del provvedimento, interessano entrambe ([20]). Potrebbe accadere che lo stesso cittadino abbia delegato due diverse organizzazioni a rappresentarlo per le due aree. Il conflitto che ne deriverebbe può essere risolto attraverso una proprietà della delega che assegna ad ogni persona o organizzazione delegata un numero di credito. Nel caso di conflitto la rappresentanza del voto verrebbe assegnata al delegato con numero di credito maggiore.

Ovviamente, il semplice modello proposto deve confrontarsi con una lunga serie di eccezioni, perplessità e quant'altro, sia di ordine politico che di carattere meramente tecnico, prima di potersi qualificare come uno dei modelli «credibili» per una nuova forma di partecipazione e rappresentanza. In questo senso, un caso particolarmente interessante che può subito analizzarsi nei tratti essenziali è quello della segretezza del voto e della delega.

Non vi è dubbio che quando il voto viene espresso direttamente da un cittadino non titolare di deleghe esso possa essere dato, se previsto, in modo segreto. Per segreto si intende che in nessun modo, mai, qualcuno può risalire all'abbinamento «voto espresso-cittadino». In effetti, tale abbinamento per i voti espressi in modalità segreta non esiste fisicamente nel sistema informatico, pur essendo possibile verificare in ogni momento i voti attribuiti alla stregua, ma con maggiori garanzie, di quanto avviene nella successiva verifica dei dati elettorali attraverso un secondo spoglio delle schede utilizzate nei seggi. Nel prossimo capitolo si descriverà puntualmente e comparativamente proprio l'attribuzione del voto segreto che, rappresentando il caso più complesso, ricomprende tutti gli altri.

Discorso più articolato va fatto per le deleghe che, almeno in prima approssimazione, possono considerarsi di tre tipi: pubbliche, riservate e segrete. Un cittadino può scegliere liberamente come qualificare la delega che sta attribuendo.

Una delega è di tipo pubblico quando chiunque, interrogando il sistema informatico, ha la possibilità di vedere che per una o più aree tematiche il signor A ha delegato il signor B.

Una delega è di tipo riservato quando l'abbinamento tra delegato e delegante è noto soltanto ad un gruppo ristretto di persone: al minimo, il gruppo è costituito soltanto dai due interessati.

Infine, una delega è di tipo segreto quando viene espressa in modo tale che in nessun modo, mai, qualcuno possa risalire al delegante, neppure il delegato stesso.

Ovviamente, la scelta di un tipo di delega piuttosto che di un'altra ha delle conseguenze. Infatti, poiché al sistema informatico sono noti soltanto gli abbinamenti delegato-delegante per le deleghe di tipo pubblico e riservato, soltanto a chi fa ricorso a questo tipo di delega è consentita l'estrema libertà di revoca e modifica cui si è fatto sinora riferimento. Chi esprime una delega di tipo segreto, invece, per evidenti motivi di impossibilità di verificare la coerenza delle operazioni compiute (come si fa ad essere certi che proprio la delega del signor X viene revocata, dal mo-

mento che è finita in un calderone indistinto di deleghe segrete?), può modificare la sua delega soltanto in momenti ben precisi. Si può infatti pensare che su base periodica uguale per tutti, ad esempio annualmente ([21]), scada il mandato relativo alle deleghe segrete e per tutti si riapra la possibilità di attribuire per la prima volta, di riconfermare, di modificare o di revocare la delega di tipo segreto.

In definitiva, un cittadino che volesse conoscere la situazione delle deleghe attribuite al signor A dovrebbe interrogare via Internet il relativo sistema informatico e otterrebbe essenzialmente le seguenti informazioni: il signor A ha le deleghe pubbliche dei signori B, C e D, ha 100 deleghe riservate e 10 deleghe segrete.

In questo modello, che tende a conservare per ognuno flessibili modalità di partecipazione e rappresentanza, va ben tutelata la figura del delegato almeno perché nessuno subisca la violenza di una delega non voluta. In questo senso, prima di tutto, il modello deve prevedere, ed il sistema informatico deve gestire, l'elenco dei cittadini o organizzazioni che espressamente accettano di essere delegati di altri. Inoltre, l'iscrizione a tale elenco deve essere qualificata attraverso l'esplicita segnalazione del tipo di delega che si è disposti ad accettare. In tal modo se un delegato, ad esempio, non vuole accettare deleghe di tipo segreto è nella piena libertà di farlo. Inoltre, per le deleghe di tipo pubblico e riservato, va contemplata la possibilità per il delegato di non accettare una delega o, successivamente, di ripudiarla.

L'accettazione di un tipo di delega invece di un'altra non è indifferente per la pubblicità che il voto espresso dal delegato può assumere ([22]). Sembra credibile che se un delegato avesse solo deleghe di tipo pubblico o riservato il voto che egli esprime possa, a sua scelta, o essere pubblico o comunicato riservatamente ai deleganti. Se invece ha anche deleghe del tipo segreto, necessariamente il suo voto deve essere pubblico. Ciò in ottemperanza al principio fondamentale della trasparenza, sottostante al modello, che pretende che ogni cittadino deve avere la massima visibilità sulle opinioni pubbliche e le scelte operate da chi è stato da lui delegato.

Un meccanismo di deleghe così articolato è tale per cui si può prevedere che nel fisiologico sviluppo del sistema e nel rispetto delle prerogative individuali di ogni cittadino, si pervenga ad una spontanea e sostanziale convergenza verso grandi ed omogenee rappresentanze. È forse riconoscibile in questi spazi di aggregazione il ruolo nuovo che, meglio di ogni altra organizzazione, potrebbe essere svolto in futuro dagli attuali partiti.

In questo scenario, le attuali assemblee rappresentative, di molto ridotte nel numero dei partecipanti ([23]), elette con metodo proporzionale senza vincolo di mandato e con logiche non soltanto legate al territorio, non sarebbero più chiamate a deliberare su una infinità di piccole e grandi questioni, ma rivestirebbero essenzialmente un ruolo di autorità di indirizzo, regolazione, controllo e garanzia. In questa nuova veste, potrebbe effettivamente rappresentare la più autorevole espressione della società civile. Ad ognuna di esse, ad esempio, relativamente al proprio dominio (la nazione, la regione, il comune), potrebbe essere attribuita l'individuazione delle grandi aree tematiche sulle quali i cittadini possono esprimere le deleghe. Ad esse competerebbe la qualificazione e l'interpretazione delle questioni da ritenersi di rilevante interesse generale e quindi da sottoporre a particolari procedure o garanzie. In questo contesto, anche se l'importanza del tema meriterebbe ben più approfondita riflessione, potrebbero essere i garanti politici dei diritti e delle libertà fondamentali dell'uomo, quali la libertà di espressione, di riunione, di culto che andrebbero per l'appunto salvaguardate sottraendole ad ogni tentazione di «dittatura della maggioranza». Sicuramente dalle assemblee, proprio in quanto organi di garanzia, potrebbero dipendere i sistemi informatici preposti al buon funzionamento di tutto il sistema. A questo proposito, andrebbe probabilmente nominato un apposito Comitato di garanzia tra i membri delle assemblee per controllare la coerenza, l'affidabilità e la sicurezza delle informazioni trattate e dei programmi che le elaborano. Più controversa, o comunque soggetta a maggior riflessione, potrebbe essere l'attribuzione ad esse della formazione dell'ordine del giorno e del calendario dei lavori.

Per quanto riguarda l'elezione dei membri delle assemblee, come detto rigorosamente eletti con metodo proporzionale, il meccanismo di voto è ancora elettronico ed ogni cittadino deve esprimerlo personalmente e segretamente senza che sia utilizzabile nessun meccanismo di delega.

In effetti, un'Assemblea così eletta, e sollevata dall'assunzione di decisioni a carattere «operativo», è destinata ad impegnarsi sulle grandi questioni di indirizzo politico e pertanto non diviene più appetibile a coloro che concepiscono il mandato elettorale in Parlamento e nelle assemblee regionali e comunali in termini di puro esercizio del potere.

Per concludere la sommaria rappresentazione del modello, può essere forse utile ricapitolarne brevemente le caratteristiche attraverso un esempio.

Supponiamo che il Governo presenti un disegno di legge e che la Camera dei deputati, riconfigurata come sopra delineato con riguardo alla composizione ed ai compiti, abbia avuto anche il mandato di fare l'ordine del giorno ed il calendario dei lavori nel rispetto di norme generali fissate. Pertanto, essa iscrive il disegno di legge all'ordine del giorno attribuendolo ad un'area tematica; definisce, sempre in armonia con norme prestabilite, i tempi della lavorazione e pubblica il disegno di legge via Internet. I cittadini e i gruppi interessati al disegno di legge si mobilitano per effettuare gli emendamenti che ritengono più opportuni. La fase di preparazione degli emendamenti può richiamarsi a quanto già esposto nella nota 19. Per poter presentare l'emendamento però, è necessario che esso sia firmato da un numero ben definito di richiedenti. Pertanto, tutti coloro che vogliono presentare emendamenti devono assicurarsi di raggiungere tale numero. Per farlo conteranno le firme di singoli cittadini per una unità e le firme di soggetti delegati per tante unità quante sono le deleghe possedute in quel momento relativamente all'area tematica cui il disegno di legge afferisce. Se il *quorum* viene raggiunto, l'emendamento viene presentato e può essere votato. Ovviamente, se tra il momento della presentazione e la votazione dovesse venire a mancare il numero di firmatari necessari per sostenere l'emendamento, lo stesso si intenderebbe ritirato.

Per concludere, vale forse la pena notare che il modello proposto potrebbe enormemente avvantaggiarsi, nella definizione di molte procedure che ne dovrebbero regolare il funzionamento, di tutta la grande esperienza accumulata nella gestione delle assemblee rappresentative.

4 - *La tecnologia informatica a supporto dei nuovi modelli di partecipazione e rappresentanza*

Le componenti tecnologiche necessarie per la concreta realizzazione di nuovi modelli di partecipazione e rappresentanza democratica ispirati a quanto sinora illustrato sono tutte assolutamente già disponibili.

In effetti, l'evoluzione dei sistemi di produzione e delle possibilità di comunicazione, la ricerca di economie di velocità ancor più che di scala, l'espansione dei mercati verso una globalizzazione che vedrà nel commercio elettronico conferma e spinta propulsiva, determinano una condizione al contorno che per un verso rende disponibili a costi accettabili le tecnologie e per altro verso spingono ad aggiornare i metodi e gli strumenti della politica.

Sulle componenti tecnologiche di base del sistema — elaboratori di elevate capacità computazionali, sistemi di gestione di grandi basi di dati, reti di trasmissione a larga banda, sistemi per la sicurezza fisica e logica, interfaccia grafica per gli utenti e così via — non vale la pena soffermarsi in questo contesto, perché non avrebbero niente di specifico rispetto a quanto non venga già normalmente impiegato nei sistemi informatici di organizzazioni complesse. Nel successivo paragrafo, invece, sia pure con linguaggio divulgativo e con la dovuta sinteticità ([24]), ci si sofferma su una parte di più recente concezione la cui comprensione è però fondamentale per fugare ogni dubbio circa la sicurezza, il rispetto della *privacy*, l'assenza, almeno per quanto riguarda il sistema proposto, della materializzazione del «grande fratello». Inoltre, per chi non ha confidenza con i meccanismi di funzionamento dei sistemi a chiavi pubbliche, può essere un'utile introduzione alla comprensione del capitolo successivo.

4.1 - *La crittografia a chiavi pubbliche, la firma digitale, l'autorità di certificazione*

La crittografia, cioè l'insieme delle teorie e delle tecniche che permettono di cifrare un testo in chiaro, ottenendo un testo segreto (crittogramma), attraverso l'impiego di una chiave di cifratura e di decifrare un crittogramma utilizzando una chiave di decifratura, ha una storia lunga almeno quanto quella della scrittura stessa ed è stata la fidata complice nell'intessere intrighi, nel trasportare informazioni segrete in tempo di pace e, soprattutto, in ogni guerra ([25]). Oggi, oltre a continuare a svolgere le stesse funzioni, la crittografia è alla base dei sistemi per realizzare il commercio elettronico, la firma digitale dei documenti e la riservatezza delle informazioni che ogni utente gestisce e si scambia anche attraverso reti aperte quali Internet.

I sistemi di crittografia attualmente adottati per realizzare tali funzioni sono tutti riconducibili a due grandi famiglie: a chiave simmetrica e a chiave asimmetrica.

La prima modalità, a chiave simmetrica, è quella più antica e più efficiente in termini computazionali ma sostanzialmente inutilizzabile da gruppi numerosi o a fini di autenticazione della paternità di un documento (firma digitale). In pratica, si basa sull'uso della stessa chiave per effettuare sia l'operazione di cifratura che quella di decifratura. Di conseguenza, se due persone vogliono scambiarsi un messaggio segreto in

questa modalità entrambe devono conoscere la stessa chiave ([26]). Se poi i soggetti che devono scambiarsi messaggi sono 10, ecco che le chiavi complessivamente in circolazione diventano 45. Per una popolazione di 1000 utenti le chiavi in circolazione sono circa mezzo milione ([27]). Pertanto, tale sistema non è praticamente gestibile nel caso di molti utenti anche se si volesse utilizzarlo soltanto per erogare un servizio di cifratura/decifratura. È invece molto utilizzato per la cifratura di canali di comunicazione o di documenti in combinazione con il sistema a chiavi asimmetriche.

Proprio per trovare soluzione alla trasmissione di un numero segreto (la chiave del sistema simmetrico di cui abbiamo appena detto) attraverso un canale trasmissivo insicuro, due matematici americani «giocando» con i numeri posero le basi della crittografia a chiavi pubbliche ([28]).

Il nuovo sistema si basa sull'attribuzione ad ogni utente di una coppia di chiavi: una privata, da conservare in modo segreto e di cui è a conoscenza soltanto l'utente, ed una pubblica che va resa nota a tutti ([29]). Le due chiavi sono complementari, nel senso che qualsiasi messaggio cifrato con una chiave può essere decifrato solo e soltanto con l'altra e viceversa. In tal senso ogni coppia è unica: non esiste nessun'altra chiave che possa sostituirsi ad una della coppia. In sostanza, ad una chiave pubblica corrisponde una ed una sola chiave privata e viceversa. In questo modo la gestibilità del sistema è assolutamente possibile, dato che ogni utente effettua le operazioni di cifratura/decifratura dei documenti e di firma digitale utilizzando una coppia di chiavi ([30]). Pertanto una popolazione di 1000 utenti utilizzerà complessivamente soltanto 1000 coppie di chiavi.

L'altra proprietà caratteristica del sistema è l'impossibilità materiale che, nota una chiave della coppia, si possa ricavare l'altra. Quest'ultimo concetto è fondamentale ai fini della tranquillità di ogni utente circa l'impossibilità che qualcun altro, amico o servizio segreto, possa per questa via, per via informatica cioè, impadronirsi di un suo segreto o firmare al suo posto. L'impossibilità materiale di risalire all'altra chiave o, analogamente, di decifrare maliziosamente il messaggio, è collegata al fatto che assumendo la chiave di cifratura di 1024 bit, come è ormai consuetudine, scovare la chiave abbinata comporta l'esplorazione di un numero di chiavi pari a circa 10^{306} (cioè di un numero decimale formato da 307 cifre). È ovvio che nessun essere umano riesca a concepire qualche cosa di fisicamente misurabile con un numero tanto grande. Al puro fine di dare una sensazione, peraltro particolarmente evocativa per l'immaginario collettivo, l'età accreditata dell'universo è di 18 miliardi di anni che,

pur misurata in secondi, corrisponde quindi *soltanto* a circa 10^{17} secondi (cioè ad un numero decimale formato *soltanto* da 18 cifre) ([31]).

Date le premesse vediamo come sia semplice effettuare l'operazione di cifratura e decifratura di un documento ipotizzando che il signor Rossi voglia inviare un documento segreto al signor Bianchi, in modo tale cioè che soltanto il signor Bianchi riesca a leggerne il contenuto.

Il signor Rossi, attraverso il suo personal computer, recupera la chiave pubblica del signor Bianchi e la utilizza per cifrare il documento. In questo modo può spedirlo tranquillamente anche sulla rete Internet poiché nessun altro può decifrarlo a meno dell'interessato. Il signor Bianchi riceve il documento e attraverso il suo personal computer, utilizzando la sua chiave privata — l'unica matematicamente corrispondente alla sua chiave pubblica — procede a decifrare il documento ([32]).

Con altrettanta semplicità il signor Bianchi può inviare, diciamo al signor Verdi, un documento sottoscritto. Per fare questa operazione è sufficiente che il signor Bianchi usi la sua chiave privata per cifrare il documento e proceda poi all'invio a Verdi (o a chiunque altro abbia voglia). Poiché il messaggio così cifrato è interpretabile solo e soltanto dalla corrispondente chiave pubblica di Bianchi, il signor Verdi, per verificare l'autenticità del documento, non deve far altro che recuperare la chiave pubblica di Bianchi e provare con essa a decifrare il documento. Se l'operazione si conclude con successo, il signor Bianchi non potrà disconoscerne la paternità essendo dimostrabile l'autenticità e l'integrità del documento pervenuto ([33]).

Le due operazioni di cifratura e firma possono ovviamente essere abbinate insieme in modo da garantire la segretezza, l'autenticità e l'integrità di quanto scambiato. Per realizzare ciò il signor Rossi deve sottoscrivere attraverso la sua chiave privata il documento da inviare a Bianchi e quindi utilizzare la chiave pubblica di quest'ultimo per renderlo incomprensibile a chiunque altro. In ricezione, il signor Bianchi prima di tutto decifrerà il contenuto del documento con la sua chiave privata e poi verificherà la firma utilizzando la chiave pubblica di Rossi.

Dal punto di vista dell'utente tutte queste operazioni vengono realizzate semplicemente attraverso la selezione delle opportune funzioni («firma», «cifra», «firma e cifra») sulla interfaccia grafica del proprio computer. In realtà, prima di arrivare a questo punto, devono essere risolte alcune questioni fondamentali.

In primo luogo, chi garantisce ai vari signor Rossi, Bianchi e Verdi che le chiavi pubbliche, recuperate tipicamente via Internet, siano effettivamente quelle dei legittimi proprietari e non piuttosto quelle di

qualche impostore che si è impersonificato in altri? E poi, chi mi assegna la chiave privata? e come faccio ad essere sicuro che non mi venga catturata quando mi collego al sistema?

Alla prima domanda la risposta è: l'Autorità di certificazione. Si tratta cioè di una terza parte fidata che applica procedure rigorose, verificabili, trasparenti ed aderenti a standard di qualità internazionali in ogni fase della sua attività. Un utente, per prima cosa, dovrà registrarsi presso un'Autorità di certificazione riconosciuta utilizzando le procedure previste per la sua certa identificazione. Successivamente, come si preciserà oltre, l'utente genera autonomamente la coppia di chiavi (pubblica e privata) e richiederà all'Autorità la certificazione della propria chiave pubblica. L'autorità provvederà quindi a generare e sottoscrivere un certificato, che pertanto non è ripudiabile, contenente tra le altre informazioni la chiave pubblica dell'utente. Tale certificato verrà inviato all'utente e sarà pubblicato nei servizi di indirizzario dell'Autorità ed eventualmente replicato in altri siti autorizzati. Pertanto, la verifica della chiave pubblica va effettuata a cura degli utenti consultando i certificati così rilasciati e pubblicati.

Per quanto riguarda la sicurezza della propria chiave privata va subito precisato che la coppia di chiavi, cioè la chiave pubblica e quella privata, viene generata autonomamente, al di fuori di qualunque interferenza o controllo, dall'utente su di un apposito dispositivo in suo possesso. Si tratta tipicamente di particolari *smart card* o di così dette *cripto card*, ormai della dimensione di una comune carta di credito, specializzate per l'autonoma generazione e memorizzazione della coppia di chiavi e per l'apposizione della firma digitale. Sono dispositivi, certificati contro ogni forma di effrazione, che non consentono alla chiave privata di essere usata al di fuori della carta stessa. L'utente accede alle funzionalità della carta previo inserimento di un PIN (*Personal Identification Number*) da lui impostato in fase di inizializzazione della carta. In definitiva, mentre la chiave pubblica viene inviata all'Autorità per la necessaria certificazione, la chiave privata, dalla sua generazione in poi, non lascia mai la propria carta. In caso di smarrimento o furto della carta, anche se il sistema di protezione attraverso il PIN funziona in modo tale che dopo un limitato numero di tentativi la carta si disattiva, è opportuno fare immediatamente una comunicazione all'Autorità di certificazione che da quel momento sospende o revoca il corrispondente certificato, impedendo a chiunque di utilizzare in modo fraudolento la carta.

5 - *Una procedura per l'attribuzione elettronica del voto segreto*

La maggior parte delle operazioni descritte nel modello presentato al capitolo 2 sono attuabili senza un'attenzione esasperata alla riservatezza. Ve ne sono però alcune che la richiedono come, ad esempio, l'espressione di voti o deleghe segrete. Comunque, più in generale, non ci si può esimere dall'affrontare il problema di esprimere in modo anonimo, e quindi segreto, il proprio voto. Anche perché, essendo questo il caso di maggior complessità, una volta che sia stato risolto in modo soddisfacente rende automaticamente soddisfatte tutte le altre condizioni.

Si ritiene altresì necessario precisare che pur essendo la sicurezza del sistema di votazione elettronica assai robusta anche sotto il profilo dell'anonimato, il sistema non va confrontato con un'ipotetica sicurezza assoluta, ma piuttosto relativamente alla sicurezza dei sistemi manuali sinora adottati ed accettati. Si precisa questo concetto non tanto per anticipare osservazioni sugli aspetti eventualmente ritenuti «deboli» della soluzione informatica, quanto per sottolineare che l'assenza di perfezione, inevitabilmente presente in ogni realizzazione umana, sia pure informatica, non deve allontanarne o pregiudicarne l'introduzione.

Problema diverso, ma altrettanto importante da richiamare, è la difficoltà di molti decisori di comprendere il linguaggio, i metodi e le regole dell'informatica e, come ben si sa, niente spaventa di più dell'ignoto.

Nel caso specifico delle votazioni, sono ben noti i brogli, gli errori e quant'altro caratterizza ogni elezione. Non vale la pena in questa sede di passarli in disamina, ma bisogna tenerli presente quando si faccia il confronto con il sistema informatico.

La soluzione proposta, indicata nel seguito come "*Procedura informatica*", è ancora una volta essenzialmente esemplificativa di che cosa è possibile fare. Una riflessione più attenta, stimolata da segnali di interesse intorno a queste tematiche che portassero alla costituzione di gruppi di lavoro interdisciplinari a forte motivazione, sicuramente potrebbe produrre soluzioni di maggior efficacia.

Nel seguito, si riportano su due colonne la procedura attualmente utilizzata per effettuare le votazioni presso i seggi delle circoscrizioni e la corrispondente procedura informatica. In modo generico, si è utilizzata l'espressione "*Autorità sovraintendente le votazioni*" per indicare un organismo fidato, sopra le parti, costituito, facendo riferimento al modello del capitolo 2, ad esempio, da un comitato eletto dall'Assemblea rappresentativa e da membri scelti di altri organi costituzionali.

PROCEDURA ATTUALE	PROCEDURA INFORMATICA
Il cittadino:	**Il cittadino:**
riceve il certificato elettorale con l'indicazione del seggio presso cui recarsi a votare;	riceve sul proprio computer ([34]) l'avviso di votare per elezioni eseguite in modalità segreta e la scheda elettronica ([35]) per esprimere il voto;
si presenta al seggio elettorale presentando un documento di riconoscimento valido;	verificata l'autenticità della scheda elettronica, aggiunge ad essa il suo voto;
	cifra il tutto con la chiave pubblica dell'autorità e firma l'intero pacchetto;
	invia la scheda elettronica così compilata all'autorità;
Il personale del seggio:	**L'autorità sovraintendente le votazioni:**
verifica attraverso il documento di riconoscimento l'identità del cittadino;	verifica, attraverso la chiave pubblica del cittadino, l'autenticità della firma apposta al pacchetto ricevuto e quindi l'identità del cittadino;
controlla che sia presente nelle liste dei votanti per quel seggio; in caso affermativo firma il registro per attestare la partecipazione al voto;	controlla che sia presente nella lista dei chiamati al voto; in caso affermativo firma sull'elenco elettronico per attestare la partecipazione al voto;
restituisce parte del certificato elettorale, timbrato e firmato;	invia una ricevuta di ritorno firmata;
consegna la scheda di votazione aperta e certificata attraverso un timbro e la firma autografa del presidente del seggio (e una matita!)	-
Il cittadino:	
compila la scheda esprimendo le preferenze di voto;	-
riconsegna la scheda chiusa;	

Il personale del seggio:	
riconsegna il documento d'identità;	distrugge la firma apposta al pacchetto che in questo modo diviene anonimo;
immette la scheda nell'urna;	salva in banca dati la scheda elettronica ormai anonima;
a chiusura delle votazioni procede all'apertura delle schede attribuendo manualmente le preferenze di voto espresse;	a chiusura delle votazioni, procede all'apertura delle schede attribuendo elettronicamente le preferenze di voto espresse;
custodisce le schede ed i registri delle presenze al voto facendoli poi confluire nei centri di raccolta presso le Prefetture.	firma le schede con la sua chiave e con quella di altro soggetto istituzionale in modo che vengano conservate senza possibilità di modifiche per ogni possibile verifica successiva.

Si intuisce facilmente che la procedura di voto elettronico segreto appena descritta, oltre che molto più efficiente, è anche più sicura di quella attuale, nel senso che, ad esempio, non si presta ad una lettura maliziosa delle schede che consenta di risalire alla preferenza espressa dal cittadino. In comune con quella attuale ha però la caratteristica di fidarsi degli operatori che intervengono nel processo di votazione. Come è noto, nel caso delle attuali votazioni, essi sono quantomeno il Ministero degli Interni, le prefetture, i presidenti e gli scrutinatori di seggio, i rappresentanti delle liste. Nella procedura di votazione elettronica precedentemente indicata, gli operatori possono genericamente essere individuati nell'autorità sovraintendente le votazioni. Per quanto riguarda la segretezza del voto qualcuno allora potrebbe non fidarsi del fatto che le firme delle schede una volta controllate vengano eliminate e che quindi altri possano, sia pure attraverso un procedimento laborioso e che coinvolge la conoscenza di diverse chiavi segrete, la manomissione del software e estese complicità tra tutti i tecnici addetti al controllo del sistema informatico, risalire all'associazione con la scheda elettronica che riporta il proprio voto. La soluzione a questo problema è comunque nota e fa riferimento all'algoritmo brevettato da Schaum (vedi [Schaum 96]) per realizzare la cosidetta *blind signature* nelle transazioni economiche per via elettronica. Nella nota ([36]) si fornisce una breve descrizione di tale algoritmo che, se si ritenesse necessario, potrebbe essere introdotto nella procedura.

6 - *Conclusione*

La convergenza della tecnologia informatica, televisiva, telefonica, satellitare e di Internet è un processo inarrestabile e già a buon punto di realizzazione. Le aziende più reattive all'innovazione saranno pronte a cogliere rapidamente questa opportunità per trarne il massimo vantaggio competitivo. Contemporaneamente, la normativa sul documento e la firma elettronica avrà avuto coronamento attraverso la disponibilità di adeguate autorità di certificazione e l'innesco di un circolo virtuoso nello scambio di informazioni, trasparenti ed efficaci, delle pubbliche amministrazioni tra loro e con i cittadini.

In questo quadro, la politica, quella interessata alla partecipazione ed alla rappresentanza di tutti gli interessi, dov'è? che progetti fa? È certamente necessario, e le iniziative intraprese vanno in tale direzione, rendere efficiente il Parlamento nel conseguimento della sua missione attraverso il recupero, accumulato nel tempo, del divario tecnologico ed attrezzandolo per competere da una parte con i gruppi di interesse e dall'altra con il governo. Ma tutto ciò, è sufficiente per conservare al parlamentarismo la sua centralità? oppure, vanno progettate soluzioni radicalmente nuove, fino ad elaborare modelli in cui i cittadini scelgono liberamente e continuamente per che cosa partecipare direttamente e per che cosa lasciarsi rappresentare?

La necessità di un dibattito ed una riflessione ampia ed articolata intorno a questi temi s'impone; affrontarla esclusivamente nell'alveo di una cultura puramente storico-giuridico-umanistica, senza una completa integrazione con quella tecnologica, sarebbe un grave errore, equivalente, per usare un'espressione commerciale, alla rinuncia di rimanere sul mercato in posizione dominante o almeno rilevante.

In questo lavoro si è presentato, a fini esemplificativi e di studio, proprio un modello per una nuova forma di partecipazione e di rappresentanza. È ovvio che numerosi possono essere i miglioramenti da apportarvi, sia sotto il profilo funzionale che tecnologico. Così come, pur rimanendo sulla linea di un uso intensivo della tecnologia, possono essere elaborati altri modelli, alternativi a quello presentato nei contenuti e nelle finalità.

In ogni caso, per concludere, qualunque fosse il modello di riferimento, si porrebbe il problema di vagliarlo nel funzionamento reale, successivamente ai dibattiti ed alle analisi concettuali, alle simulazioni e alle prove di laboratorio.

Da questo punto di vista, un approccio potrebbe essere quello di partire da un piccolo campione di comuni, di diversa grandezza, distribuiti

su tutto il territorio nazionale. Ad essi, come incentivazione per la conduzione della sperimentazione, potrebbero essere garantite formule agevolate per finanziare gli investimenti da effettuare: nelle strutture pubbliche (in termini di un forte incremento nella disponibilità di computer nelle scuole, biblioteche, sale comunali aperte al pubblico), in quelle private (in termini, ad esempio, di incentivi all'ammodernamento tecnologico alle aziende che rendessero disponibile, agli scopi della sperimentazione, delle finestre di impiego delle proprie apparecchiature al proprio personale), ai cittadini stessi (ad esempio, incentivi agli abitanti del comune per l'acquisto di attrezzatura informatica utile alla sperimentazione), alle scuole (per l'erogazione di corsi di alfabetizzazione informatica alla popolazione) e così via. Per non incidere sugli Statuti e sulle norme comunali, la sperimentazione, almeno nella sua fase iniziale, potrebbe essere basata su una sorta di «patto d'onore» tra il consiglio, la giunta comunale e la cittadinanza. In base a tale patto, il consiglio e la giunta comunale:

– eleggono un rappresentante per la maggioranza ed uno per l'opposizione, che a loro volta nominano un presidente: si realizza, in pratica, una sorta di collegio arbitrale «politico». Il collegio, così formato, ha l'incarico di vigilare, eventualmente servendosi delle opportune consulenze, sulla regolare esecuzione di tutte le operazioni e di risolvere le controversie che dovessero nascere;

– stabiliscono gli argomenti da deliberare attraverso il modello che è stato prescelto per condurre la sperimentazione;

– accettano di fare oggetto di una propria tempestiva deliberazione, senza apportare alcun correttivo, la scelta operata dalla cittadinanza.

I presidenti dei collegi formati nei comuni, osservatori delegati dalle assemblee regionali e dal Parlamento effettuano un'opera di monitoraggio complessivo sull'andamento della sperimentazione. A fronte dell'esito positivo di questa prima fase, che potrebbe durare circa due anni, si stabilirebbero le linee di sviluppo necessarie per un graduale allargamento del nuovo modello di partecipazione e rappresentanza agli altri comuni, alle regioni ed a tutta la nazione.

Note

(1) La legge 15 marzo 1997, n. 59 (Delega al governo per il conferimento di funzioni e compiti alle Regioni ed enti locali, per la riforma della pubblica amministrazione e per la semplificazione amministrativa), all'art. 15, comma 2, afferma quanto segue: «Gli atti, dati e documenti formati dalla Pubblica Amministrazione e dai privati con strumenti informatici, sono validi e rilevanti a tutti gli effetti di legge. I criteri e le modalità di applicazione del presente comma sono stabiliti, per la Pubblica Amministrazione e per i privati, con specifici regolamenti da emanare entro centottanta giorni dalla data di entrata in vigore della presente legge ai sensi dell'articolo 17, comma 2, della legge 23 agosto 1988, n. 400. Gli schemi dei regolamenti sono trasmessi alla Camera dei deputati e al Senato della Repubblica per l'acquisizione del parere delle competenti commissioni».

(2) Vedi, in particolare, [Chimenti 92] e [Riddell 98].

(3) Il sito della Camera dei Deputati è raggiungibile all'indirizzo www.camera.it; quello del Senato all'indirizzo www.senato.it; infine, entrambi sono raggiungibili all'indirizzo www.parlamento.it.

(4) I dati riportati sono tratti da [Mandelli 98] sul sito dell'Università Bocconi, Osservatorio Internet Italia, all'indirizzo www.sda.uni-bocconi.it/oii/. Allo stesso studio sono riferiti anche i successivi dati relativi all'uso di Internet.

(5) Si tratta del decreto del Presidente della Repubblica 10 novembre 1997, n. 513 (Regolamento dell'articolo 15, comma 2, della legge 15 marzo 1997, n. 59, in materia di formazione, archiviazione e trasmissione di documenti con strumenti informatici e telematici) e della bozza di decreto del Presidente del Consiglio dei ministri (ai sensi dell'articolo 3, comma 1, del decreto del Presidente della Repubblica 10 novembre 1997, n. 513).

(6) Da [AAVV 88], p. 26.

(7) «Ogni membro del Parlamento rappresenta la Nazione ed esercita le sue funzioni senza vincolo di mandato».

(8) Da [Bobbio 95], p. 12.

(9) Vedi Norberto Bobbio, «Rappresentanza ed interessi» e Gianfranco Pasquino, «Rappresentanza e decisione» in [AAVV 88].

(10) Dall'intervento di Pietro Scoppola in [Camera 98], p. 36.

(11) Dall'intervento di Tom R. Burns in [Camera 98], p. 62.

(12) Ancora dall'intervento di Tom R. Burns in [Camera 98], pp. 52 e 53; sullo stesso tema vedi anche [Riddel 98].

(13) Dall'intervento di Tom R. Burns in [Camera 98], p. 72.

([14]) Vedi ad esempio [Arterton 87]. Sull'argomento, comunque, vi comincia ad essere interesse, come testimonia il sito della Teledemocracy Action News + Network, raggiungibile all'indirizzo www.auburn.edu/tann/tann2.

([15]) Da «Il futuro della democrazia», in [Bobbio 95], p. 14.

([16]) Da «Il futuro della democrazia», in [Bobbio 95], p. 19.

([17]) Da «Democrazia rappresentativa e diretta», in [Bobbio 95], p. 49.

([18]) Più precisamente, sono identificabili con certezza — non "ripudiabili" — i documenti, le comunicazioni e le transazioni che egli firma elettronicamente.

([19]) Così in [Manacorda 93] come citato in [Rodotà 93] p. 592 e ss. «Supponiamo che in un'associazione di cittadini si voglia avanzare una proposta di delibera di iniziativa popolare al proprio comune, possibilità consentita da diversi statuti comunali. Coloro che lanciano questa idea possono, tramite un personal computer in rete, diffonderla ad altri associati (per esempio utilizzando una posta elettronica a gruppo chiuso), chiedendo a tutti di pronunciarsi con commenti, integrazioni, osservazioni. Questo può essere fatto con la conferencing in cui tutti, con i loro personal computers in rete, possono appunto inviare messaggi, commenti, integrazioni, osservazioni. Tutti i partecipanti alla conferenza hanno la possibilità di vedere sul loro schermo questi «interventi», che possono essere nominativi o, volendo, anonimi. I relatori, resisi conto che la proposta iniziale è bene accolta, possono formulare una bozza iniziale di delibera, che viene vista da tutti gli altri sui loro schermi. Utilizzando una tecnica di *co-authoring*, la bozza iniziale appare su una metà dello schermo, mentre sull'altra metà appaiono le integrazioni e le modifiche inviate dagli altri «coautori». Gli autori della bozza iniziale possono accettare o meno le modifiche proposte e inserirle nella bozza. Tutto il processo è comunque molto trasparente, perchè appare sugli schermi di tutti coloro che partecipano a questa sorta di riunione a distanza e in tempo differito. Se gli autori hanno delle opzioni da presentare ai partecipanti alla riunione, possono sottoporle al voto elettronico, che verrà inviato sempre tramite il proprio personal computer, eventualmente accompagnato dalle motivazioni. Quando gli autori ritengono che la bozza sia nella sua forma finale, possono sottoporla al voto finale dei loro colleghi, che così avranno partecipato alla stesura in modo certamente più collettivo e più agevole che non partecipando di persona a molte riunioni». Il caso riportato, prescindendo dalla particolare finalizzazione dell'esempio fatto, è esemplificativo di possibili modalità generali di interazione di gruppo atte a definire il contenuto di un nuovo provvedimento o di un emendamento ad un disegno di legge in discussione.

([20]) Questo caso è simile a quanto già avviene presso la Camera per l'esame congiunto di un provvedimento da parte di due Commissioni.

([21]) La scelta della periodicità con cui far cessare il mandato relativo alle deleghe segrete deve rappresentare un giusto compromesso tra l'esigenza di non vincolare, in modo non modificabile, una delega per troppo tempo ad un delegato e la preoccupazione che un ricorso troppo frequente alla verifica di tali

deleghe possa portare ad una disaffezione del sistema con una mancata attribuzione delle deleghe.

([22]) In effetti, ci potrebbero essere motivi etici e politici a determinare l'accettazione di un tipo di delega piuttosto che di un altro.

([23]) Sembra decisamente opportuno che gli eletti in Assemblea non possano essere titolari di deleghe.

([24]) Queste caratteristiche espositive non consentono la puntuale disamina di ogni aspetto del problema e di tutte le procedure messe in atto per garantire la sicurezza delle operazioni effettuate. Per gli approfondimenti si rimanda alla abbondante letteratura presente sull'argomento e normalmente pubblicata in Internet. Il sito dell'Autorità per l'informatica nella pubblica amministrazione (www.aipa.it), ad esempio, contiene, oltre ai testi del decreto del Presidente della Repubblica 10 novembre 1997, n. 513 (Regolamento contenente i criteri e le modalità di applicazione dell'articolo 15, comma 2, della legge 15 marzo 1997, n. 59, in materia di formazione, archiviazione e trasmissione di documenti con strumenti informatici e telematici) e della bozza di decreto del Presidente del Consiglio dei ministri (Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici ai sensi dell'articolo 3, comma 1, del decreto del Presidente della Repubblica 10 novembre 1997, n. 513), che costituiscono di per sè un fondamentale riferimento, molti documenti interessanti a questo proposito, tra cui una monografia su «firma elettronica: tecnologie e standard» corredata da un utile appendice sui principali standard di riferimento. Sempre tra i siti italiani, è possibile trovare documenti interessanti in quello del Consiglio Nazionale del Notariato (www.notariato.it). Nei siti dei grandi produttori mondiali di soluzioni per autorità di certificazione è disponibile un'ampia presentazione delle caratteristiche tecniche dei diversi prodotti: tra questi, lungi dall'esaurire la lista, quello della Gte CyberTrust (www.gte.com), quello di Entrust (www.entrust.com), quello di Rsa Data Security (www.rsa.com). Vale poi forse la pena visitare anche il sito della VeriSign (www.verisign.com), la maggior autorità di certificazione privata al mondo, e richiedere in prova un certificato.

([25]) Tra le infinite possibilità, è possibile ricordare nell'antichità i codici di Cesare e in tempi più recenti, ad esempio attraverso la biografia [Turing 83] di Alan Turing — uno dei più grandi scienziati del nostro secolo — le tecniche utilizzate per rompere uno dei maggiori segreti della seconda guerra mondiale: il codice Enigma, il sistema di crittografia a chiave simmetrica utilizzato dall'esercito tedesco.

([26]) È questo il motivo per cui non può essere usata per attribuire in modo "non-repudiabile" la paternità del documento: almeno un altro soggetto possiede esattamente la stessa chiave.

([27]) Come è semplice verificare attraverso un processo induttivo, per N utenti sono necessarie N*(N-1)/2 chiavi simmetriche.

([28]) In [Diffie 76] è indicato l'articolo che fonda la crittografia a chiave pubblica. In [Schneier 96] si trova probabilmente la raccolta più completa di algoritmi crittografici e tecniche di *data privacy* sino ad oggi pubblicata. In [RSA 78] il lavoro fondamentale, messo a punto da Rivest R., Shamir A. e Adleman L., per quanto riguarda l'algoritmo più diffuso di firma digitale a chiave pubblica.

([29]) La realizzazione del sistema per la firma digitale di cui alla legge 15 marzo 1997, n. 59 e successivo decreto del Presidente della Repubblica 10 novembre 1997, n. 513, è basata proprio su questo meccanismo a chiave pubblica.

([30]) Anche se è ininfluente alla comprensione del discorso, è bene precisare che molto spesso si preferisce utilizzare una doppia coppia di chiavi: una dedicata alla firma e l'altra dedicata alla cifratura/decifratura. Ciò viene fatto soprattutto per assoggettare l'impiego delle chiavi a due diverse politiche; ad esempio, sulla coppia di chiavi di cifratura/decifratura è possibile prevedere (e in alcuni casi è necessario) un *key recovery*, la possibilità cioè di ricostruire la chiave in caso di smarrimento, perdita o quant'altro.

([31]) L'osservazione più pertinente a questo proposito è relativa al fatto che anche gli elaboratori elettronici possiedono potenze di calcolo non immaginabili per la mente umana e in continuo aumento. Pur tuttavia, la dimensione dei numeri trattati è talmente elevata che nessun elaboratore attuale è in grado di *rompere* una chiave di 1024 bit in un tempo utile all'appropriazione di un segreto. A titolo puramente esemplificativo, una chiave RSA asimmetrica a 768 bit richiederebbe, per essere rotta, il lavoro continuo e dedicato di un Pentium per circa un milione di anni. Inoltre, man mano che la potenza elaborativa dei computer aumenta, anche la lunghezza delle chiavi viene incrementata. Sicché già non sono praticamente più in uso chiavi asimmetriche a 512 bit e si comincia a parlare di chiavi a 2048 bit.

([32]) Nello stesso modo il signor Rossi può conservare in modo segreto un suo proprio documento. Infatti, egli può utilizzare la sua stessa chiave pubblica per cifrare un documento che potrà successivamente rileggere soltanto decifrandolo con la sua chiave privata.

([33]) In effetti, pur restando valido il principio esposto, ciò che avviene all'atto della firma digitale è leggermente più complesso. Del documento che si vuole firmare il sistema calcola attraverso una funzione hash prestabilita la cosidetta impronta. Questa impronta è costituita da una stringa di 128 o 160 bit che individua univocamente il documento originale, nel senso che a due testi diversi non corrisponde la stessa stringa. È questa impronta, cifrata con la chiave privata del firmatario, che costituisce la firma digitale del documento. In tal modo la firma prodotta risulta in relazione da una parte con il testo sottoscritto, attraverso l'impronta, e dall'altro con il firmatario, per via della chiave privata utilizzata per cifrare. Il fatto che la firma sia univocamente associata tanto al documento che al firmatario, ma che risulti fisicamente distinta, comporta il vantaggio che firma e documento possono essere memorizzate e gestite separatamente. Inoltre, ciò consente di inviare ad una *time stamping autority* la sola firma digitale del docu-

mento per l'apposizione delle marche temporali necessarie a dare certezza del momento in cui un documento è, per esempio, divenuto valido, preservando la confidenzialità del contenuto del documento. Una volta ottenuta la firma digitale essa viene normalmente aggiunta alla fine del testo del documento e l'insieme dei due viene spedito. La verifica della firma digitale viene effettuata ripetendo gli stessi passi: la chiave pubblica del firmatario viene utilizzata per decifrare la firma e ricavare l'impronta del documento che viene confrontata con quella autonomamente ricalcolata da chi effettua la verifica applicando la stessa funzione hash usata nella fase di sottoscrizione sul documento pervenuto. Se le due impronte non coincidessero saremmo in presenza di un documento contraffatto. Qualora coincidessero saremmo sicuri della autenticità e dell'integrità del documento.

([34]) Ai fini della descrizione della procedura è inessenziale che tale avviso e la scheda elettronica pervengano attraverso un sistema di posta elettronica piuttosto che ricorrendo ad una tecnologia *push* per la distribuzione delle informazioni qualificate dal cittadino come di suo interesse.

([35]) La scheda elettronica può essere costituita da un identificatore (una stringa binaria che serve ad identificare la votazione a cui si sta facendo riferimento) firmato, con la propria chiave privata, dall'autorità di sovraintendenza alle elezioni.

([36]) La *blind signature* consiste essenzialmente nel far firmare ad un operatore un messaggio senza che quest'ultimo ne conosca il contenuto. Il meccanismo alla base è il seguente: supponiamo che *A* voglia far firmare il messaggio *M* a *B* senza che *B* venga a conoscenza del contenuto di *M*. Allora *A* genera una stringa binaria *N* di opportuna lunghezza (1024 bit, ad esempio) e con questa cifra *M* ottenendo il nuovo messaggio $M^1 = M^* N^{kb}$, ove *kb* è la chiave pubblica di *B*. Ovviamente, *N* è nota soltanto ad *A* che lo ha generato. A questo punto *A* firma M^1, lo cifra con la chiave pubblica di *B* e glielo invia. *B* decifra il messaggio e verifica la firma di *A*. Tra le mani, *B* ha ora il messaggio M^1 che però essendo cifrato non gli rende possibile risalire ad *M*. Non può far altro quindi che firmare, come richiesto, il messaggio M^1 con la sua chiave privata *kpb* ed inviarlo ad *A*. Così facendo *A* ottiene il messaggio firmato $Mf=M^{1ksb}=M^{ksb*}N^{kb*ksb}=M^{Ksb*}N$. Essendo noto ad *A* il valore di *N* gli è semplice eliminarlo per ottenere esattamente il messaggio *M* firmato da *B,* M^{Ksb}. A questo punto può in modo del tutto anonimo servirsi del messaggio *M* sottoscritto da *B*.

Bibliografia

[AAVV 85/1] AA VV, *Il Parlamento tra crisi e riforma*, Milano, Franco Angeli, Centro studi e iniziative per la riforma dello Stato, 1985.

[AAVV 85/2] AA VV, *I limiti della democrazia*, a cura di Antonio Baldassarre, Bari, Laterza, 1985.

[AAVV 88] AA VV, *Rappresentanza e democrazia*, a cura di Gianfranco Pasquino, Bari, Laterza, 1988.

[Arterton 87] ARTERTON F. C., *Teledemocracy: Can Technology Protect Democracy?* Sage Library of Social Research, 1987.

[Bobbio 95] BOBBIO N., *Il futuro della democrazia*, Torino, Einaudi, 1995.

[Camera 98] AA VV, *Le assemblee elettive nella evoluzione della democrazia italiana (1978-1998),* Roma, Camera dei deputati, 1998, giornate in memoria di Aldo Moro 8-9 maggio 1998.

[Chimenti 92] CHIMENTI C., *Un parlamentarismo agli sgoccioli: lineamenti della forma di governo italiana nell'esperienza di dieci legislature*, Torino, G.Giappichelli, 1992.

[Diffie 76] DIFFIE W., HELLMAN M., *New Directions in Cryptography*, in IEEE transactions on information theory, vol. 22, 1976, p. 644.

[Di Giovine 95] DI GIOVINE A., «Democrazia elettronica: alcune riflessioni», in *Diritto e società*, numero 1, 1995, p. 399.

[Europa 96] CONSIGLIO D'EUROPA, «Risoluzione dell'Assemblea parlamentare sulla democrazia informatica», in *Il diritto dell'informazione e dell'informatica*, 1996, p. 173.

[Held 89] HELD D., *Modelli di democrazia*, Bologna, il Mulino, 1989.

[Lipow 96] LIPOW A., SEYD P., «Political Parties and the Challenge to Democracy: from Steam-Engines to Techno-Populism», in *New Political Science*, numero 33/34, autunno/inverno 1995-1996, p. 295.

[Riddell 98] RIDDELL P., *Parliament Under Pressure*, London, Victor Gollancz, 1998.

[Rodotà 93] RODOTÀ S., «La sovranità nel tempo della tecnopolitica. Democrazia elettronica e democrazia rappresentativa», in *Politica del diritto*, anno XXIV, numero 4, dicembre 1993, p. 569.

[RSA 78] RIVEST L., SHAMIR A., ADLEMAN L., «A Method for Obtaining Digital Signatures and Public-Key Cryptosystems», in *Communications of the ACM*, vol. 21, n. 2, 1978, p. 120.

[Schneier 96] SCHNEIER B., *Applied Cryptography: Protocols, Algorithms and Source Code in C*, New York, J. Wiley & Sons, seconda edizione, 1996.

[Turing 83] TURING A., Andrew H., *Alan Turing: The Enigma*, New York, Simon and Schuster, 1983.

Siti Web citati

Autorità per l'Informatica nella pubblica amministrazione www.aipa.it

Camera dei Deputati www.camera.it

Consiglio Italiano del Notariato www.notariato.it

Entrust www.entrust.com

Gte Cyber Trust www.gte.com

Osservatorio Internet Italia - Università Bocconi www.sda.uni-bocconi.it/oii

Rsa Data Security www.rsa.com

Senato della Repubblica www.senato.it

Teledemocracy Action News + Network www.auburn.edu/tann/tann2

VeriSign www.verisign.com