E-GOVERNMENT, SECURITY AND LIBERTY IN THE EU: A ROLE FOR NATIONAL PARLIAMENTS?

Juliet Lodge*

Abstract. *This paper shows how in the EU the institutionalisation of the norms, practices and procedures of accountability and transparency reflects political and legal values and commitments to sustaining them, in ways that are visible, open, embedded, just, legitimate and not arbitrary. While administrative practices and cultures uphold them to a greater or lesser degree, practice erodes them and compromises both liberty and security. First, the paper outlines the norms; then it argues that institutions are not sufficient in themselves to sustain liberty and freedom because new communication technologies (ICTs) impact on e-government and e-justice in ways that are not simply procedural. They may expedite administration and result in 'efficiency gains', but they also impact on the practices of transparency and accountability, something underscored by their appropriation by the champions of 'security'.*

Keywords: *e-government, accountability, democracy, communication technology*

The increasing use of information and communication technologies (ICTs) in public administration, commonly loosely referred to as 'e-government', raises serious questions about the role of parliaments and the nature of political legitimacy and accountability for the conduct of e-government. This presents the EU and the member governments with a paradox. On the one hand, they subscribe to the norms associated with the practice of open, transparent and accountable liberal democracy. On the other hand, they have inadvertently introduced new technologies that endanger those values. This has happened as governments have sought to increase the efficiency of their administrations, expedite the transmission of information between departments responsible for the delivery of public services, and modernise their states by getting all citizens 'online'. The message sent to citizens to persuade them to comply with this is framed in terms of efficiency and personal convenience gains. The impact on the nature and practice of democracy and political communication has been ignored. This is somewhat surprising given the simultaneous efforts by MPs and the European Parliament to ensure that any EU treaty reforms enhance the opportunity for and impact of parliamentary scrutiny by boosting co-decision and inserting procedures to enable national parliaments to play a role in EU decision-making: all in the name of liberal democratic norms and practice.

The argument for universal co-decision has been put most consistently in respect of pillar III and all the areas associated with achieving freedom, security and justice

* **Juliet Lodge** is Professor of European Studies at the Jean Monnet European Centre of Excellence, Institute of Communication Studies, University of Leeds, United Kingdom; e-mail: j.e.lodge@leeds.ac.uk

in the EU. The European Parliament's LIBE committee has paved the way for criticism of current practice, soft law measures, and a raft of steps regarding enhanced border controls, allegedly to protect and enhance the security and liberty of citizens. Vital as this is, the concerns raised about how ICTs impact upon individual and collective liberties potentially in a corrosive manner, apply beyond the boundaries of the area of freedom, security and justice (AFSJ).

In the absence of the Lisbon Treaty, national parliaments would retain their weakness in the area of internal security (AFSJ). Yet, even when considering the treaty, the (non) role of national parliaments outside the AFSJ compromises, and challenges us to rethink, the conduct of democratically accountable policymaking across the board as new technologies become the medium of choice for processing and transmitting all types of information within departments, across their boundaries, across states, and in collaboration with private and public sector bodies responsible for fulfilling public policy goals determined by elected politicians at local, regional, national and European levels.

National parliaments' and the European Parliament's powers vis-à-vis pillar III and related matters of judicial, police and migration cooperation have been progressively augmented. The Lisbon Treaty further constitutionalised the reinforcement especially of (i) the European Parliament's control powers, and (ii) the time granted for deliberation to national parliaments in respect of EU draft legislation. Collaboration between the two parliamentary layers has improved. This is beneficial for democracy and democratic accountability, but it is insufficient to ensure that liberty and security remain in balance and subject to the democratic control of elected parliamentarians because the practice of information exchange and communication is vulnerable to ICT-led insecurities and practice.

This paper begins by considering the background to ICT information exchange in the EU. Against this background, it examines the reasons for the inadequacies of institutional fixations with formal, territorial-based methods of controlling power. It then examines the current scenario of political communication. It concludes with some preliminary ideas on making digi-space amenable, at least in some part, to parliamentary control.

1. Inter-institutional information exchange in perspective

Improving the exchange of information among the EC's institutions using telematic information system exchange (as it was then called) dates back to 1974[1]. This is an important date because it coincides with two important developments in the democratisation and parlamentarisation of the EU. The first related to the implementation of the new roles of the unelected European Assembly (still not officially called the European Parliament) in respect of budgetary matters. This was the prelude to it becoming a co-equal partner with the Council of Ministers on budgetary affairs, and the point at which it began chipping away at expenditure

[1] Commission of the European Communities, Proposal for a Council Decision Relating to the Coordination of the Activities of the member states and Community Institutions with a view to setting up a Community Inter-Institutional Information System, COM(81)351 final, 6 July 1981.

on the common agricultural policy (CAP) and re-directing a greater proportion of EU revenues to other policies, like regional development. The second related to mounting pressure from MEPs and some governments of the then Nine member states to hold the first elections to the European Parliament agreed in 1975, and outlined in the Schelto Patijn and Tindemans reports. Simultaneously, the Italian communists dropped their opposition to participating in the European Assembly. This was critical for federalist Commissioner and later MEP Altiero Spinelli and a policy of small steps followed on a cross-party basis within the European Parliament (EP) to make EU executive power (the Commission and the Council) accountable to the (still to be elected) European Parliament. These heralded a transformation in the balance of power between the three key institutions in favour of openness, transparency and democratic accountability. These were seen as, and remain important to, sustaining the EU's legitimacy.

To make inter-institutional accountability work in practice, administrative reform had to accompany political reform. One of the longest and biggest complaints of MEPs had been that they were denied access to information on which the Commission (as the arm responsible for amending proposals) and the Council (solely responsible for approving them) were deliberating. Therefore, the right of the EP to give an Opinion could be negated by non-compliance on providing access to information. The idea of making information available to the EP to enhance its deliberations (and potentially therefore also meaningful oversight) over draft legislation could be dressed up in terms of enhancing public accountability of the Commission (since the Council of Ministers was to escape it for many more years) or of boosting democracy (by enabling the EP to perform the traditional role of parliaments as 'grand forum' for the people - Herman and Lodge, 1979). In practice administrators could weaken its impact but the prospect of using ICTs to expedite information sharing and exchange, even in the 1980s, opened the door to reform of bureaucratic strategies, practices and processes for exchanging information among these three institutions. Key to any action was expenditure. MEPs' attack on cutting CAP spending in favour of more diverse projects coincided with discussions over technology-led information exchange, then conceptualised very much in terms of centralised data bases and exchange hubs at supranational and national level.

Little political capital appears to have been made at the time even though ICT information exchange projects were initially funded from existing resources, and from 1982 expanded (from budget line 7711) with a specific budget from 1983. This is all the more curious in retrospect given that the arena for exploring information exchange was the CAP (CADDIA- Cooperation in Data and Documentation for Imports/Exports and Agriculture), and two pilots in the customs sector (TARIC II). In addition, the problematic technical implications of information exchange were already known: measures proposed for customs cooperation did not always match the needs of the agriculture sector and compatibility and interrelatedness issues compromised the ideals. Obtaining technical compatibility was problematic, notably regarding these systems and those covering wider Community needs likely to arise from the INSIS (interinstitutional

System for Information Services) world that overlapped with CADDIA in respect of data transmission.[2]

This focus in the 1970s and 1980s on the technical issues of information sharing and exchange (which today is reflected in the discourse on 'inter-operability'), meant that underlying democratic norms, political issues that were to preoccupy MEPs twenty years later, were not mentioned. Openness and transparency concerns became progressively hidden by a bureaucratic layer of emphasis on defining access to official documents. This in turn led to a focus on prescribing exemptions and exceptions, most of which remained subject to national rules and 'secrecy' codes. This was inevitable given that at the time the EC's scope and competence were still contested; 'security' remained taboo and the prerogative of national governments, and cooperation in justice and home affairs was conducted under political cooperation arrangements (pre-TREVI) as part of 'foreign policy' and subsequently internal market cooperation. Not until relatively recently have MEPs made the linkage explicit between technological issues and the assertion of democratic accountability for automated information and data exchange.

In the 1980s, it was taken for granted that ICTs would rationalise the procedures for the exchange of and access to information and that they in turn were bound to make the working of the institutions more efficient; boost competition, and encourage telecommunications administrations to create infrastructures for an integrated communication network. Practice reveals a different picture at variance with the ideal claimed for it, even though over thirty years ago, the governments were deliberating on many of the same problems that continue to afflict e-administration and e-government.

In its Resolution of 15 July 1974 on EC data processing policy, the Council noted its interest in joint projects. In 1979 the European Council instructed the Commission to act. In its proposal the European Council in November 1979 (COM (79) 650, it set out two principles which are reflected in modern day discourse: (i) a principle for a number of general measures seen as only being effective if carried out on a Community wide scale; and (ii) the EC institutions providing a demonstrative effect of information exchange among themselves, as a model for the transfer of information between the EC institutions and member state governments.

Following the Council Decision of 27 September 1977 instructing the Commission to study the setting up of an informatics system, a project leader was appointed in July 1978 to manage the study under the Commission's direction, and seven consultancy companies from seven different member states formed a consortium to undertake the study under a contract awarded in March 1979. The result was a ten-year development plan presented to the Commission in December 1980.

In 1981, priorities in four year plans up to 1990 were mapped out, problem

[2] Coordination of the Actions of Member States and the Commission relayed to activities preparatory to a long term programme for the use of telematics for Community information systems concerned with imports/exports and the management and financial control of agricultural market organisations: explanatory memorandum, pt. 3. COM(81)358 final.

areas identified (e.g. man-machine interface, information and training, inter-operability, standards and exchange protocol) and the need for technical transparency to users stressed. The latter was defined as end-to-end compatibility of exchange systems capable of conveying information from the new services set up between the institutions and the member states, the definition and use of exchange conventions allowing services to be supplied, and specifications for a framework to allow the new independent systems to converse with one another throughout the EC. The Commission rejected the notion of 'gateway' switching centres – one in each member state and one in the Commission – at which non-switching functions would be performed to enhance the value of information [COM 681(final) point 2, p.13]. No mention was made of citizens or the public in the context of users. It is striking that they were to be largely ignored for another decade.

Technocratised transparency versus personalised security

From the outset, there were problems within the consortium itself, difficulties at the political level and divisions at the bureaucratic levels. The rationale of boosting 'the efficiency of the Community machinery' was stressed. To that end, 'definition studies and pilot projects[3] were undertaken to identify medium and long term aims and to prepare 'general specifications for attaining them' (Explanatory Memorandum A(1)&(2) with 1982 set as the deadline for completing them, and 1986 as the point of entry into force, one year after the Isoglucose Case and the Milan summit on the Single European Act and the launch of the programme to complete the Single European Market. By 1993, ICT information exchange was common place, the EU was larger, had more competence for an expanding number of policy areas, successive IGCs had brought in treaty reforms, and the EU and member governments together were exploiting ICTs potential for enhancing cooperation among bureaucratic arms of government in the name of e-government and improved service delivery to citizens.

There was little change in the view that ICTs were a 'good thing'; and little criticism of their exponential costliness, impact on the nature of public administration, agenda setting, the feared consequences of bureaucratic engrengage (that had been a feature of anti-European federalists from the mid-1970s onwards) and parliaments. The implicit idea that technology was ideologically neutral was also initially rarely challenged as e-government was ruled out. The issues concerning the digital divide and social exclusion, therapeutic benefits of ICTs, including ambient and RFID technology, for citizens were later applauded.

ICT use for political communication purposes expanded and Data Protection codes and practices were boosted notably in the 1990s. The negative potential and consequences of ICTs became muddied by confusion over the instruments and applications of ICT enabled surveillance. 'Big Brother' became the synonym for highly diverse applications, purposes and policy goals especially in internal and external security. Public suspicion grew

[3] Study of information systems, Council Decision 77/619/EEC, OJ L 255, 6 October 1977, p.32.

over inter-operability and automated data exchange by agencies in respect of 'security' matters (police, customs, border controls, immigration, transport authorities, lawyers and social welfare offices). They were seen as threatening individual and collective liberties; as unethical, menacing intrusions into the private lives of citizens by unknown and unseen 'alien' agency officials (including those responsible for Passenger Name Record data exchange, and especially of other EU states (Tchorbadjiyska).[4] This did not accord with the public diplomacy and government rhetoric as to the advantage of information exchange for the purpose of 'good government'. Issues of data ownership and personal identity, data misuse, forensic mining and coupling of data aggravated distrust indicating that government rhetoric as to the added-value ICTs allegedly brought to individual and collective security were doubted by the public.

By the late 1990s, against this fast-changing scenario, security concerns came to focus on what could be seen by the individual. The nefarious potential for data misuse and the abuse of power was identified with the public sector adoption of ICTs. The adoption of a panoply of measures under the broad rubric of that alien trans-atlantic concept of 'homeland security', without the simultaneous adoption of parliamentary controls over the executive, changed the balance between security and liberty pitting them against each other rather than in a relationship of mutual dependence. This helps to explain a public fixation on data protection. Legitimate as this concern is, it means that the roll-out of ICTs for public policy purposes proceeded relatively unchallenged with serious implications for the conduct of democratic politics and the relevance of their normative underpinnings. Instead, legal rather than political contestation over the implementing measures took over.

Technocratised contestation

In the public sphere, the response from infant national and EU level data protection agencies was robust. Data protection honed in on data protection measures that compromised individual privacy and collective openness and transparency. It was generally accepted that it was legitimate and desirable for every administration to protect sensitive security information for the benefit of individual and collective security. Even 'open' Sweden exempted disclosure of negotiating positions and information potentially detrimental to its relations with other states.[5] But given that the EU had in 1994 begun a process of defining transparency requirements with reference to technocratically mediated 'access to documents' – the precondition of information exchange-blanket exemptions of broad categories of documents from openness and transparency codes not only contradicted the spirit of democratic openness but were deemed undesirable and contrary to the case law of the Court of Justice. This implied that:- broad categories of documents should not be exempted without explicit scrutiny as to the applicability or otherwise of one

[4] Recommendation for a Council decision concerning the accession of Bulgaria and Romania to the Convention of 26 July 1995, drawn up on the basis of Article K.3 of the Treaty on European Union, on the use of information technology for customs purposes. COM/2007/0211 final –CNS 2007/0079.

[5] Interview data, 22 June 2007.

of the grounds of exception (protecting justified interests, defence, privacy and so on); partial access must be granted to documents where non-confidential information is included; and general principles of proportionality are to be respected.(Curtin).

However, new technologies and the potential they opened for expediting information exchange and sharing, contributed to a process where the old distinctions between domestic and international politics were being eroded. They brought the normative commitment to transparency and openness into high relief. In the past, member governments had been able to justify 'exceptions' to the norm of transparency on the grounds of legitimate security concerns requiring 'secrecy'. The slippery and fuzzy arena of 'homeland security', differentiation in defence policy-making, recourse to soft law instruments and the launch of pillar II's actions in 'non-military crisis management' illustrated how the scope of exceptions would broaden in response to the imperative to combat terrorism. Not only would third states have roles unforeseen and unchallengeable by national parliaments and the European Parliament, but ICTs would facilitate erosion of protective regimes in ways not envisaged by political and administrative policy makers. The failure of parliamentary controls and accountability to keep pace with the accelerating speed of technological change and possibilities of harnessing nano-technology for security purposes is hardly surprising. Government priority-setting has escaped territorial borders and this trend is most notable in the field of ICTs for e-government.

2. The problem: inadequacies of institutional fixations with formal and territorial- based methods of controlling power

ICTs are being increasingly deployed in the name of enhancing collective territorial security without sufficient or adequate controls being made mandatory either for the technology deployed in the name of public administrative efficiency gains, or in respect of open political control over their use. The political scenario now comprises the following three elements:

1.- the new security policies of ICTs applied in domestic transactions for commerce, leisure and socio-economic welfare service access (including health, tax, licences, ID cards and even e-voting, all nominally but misleadingly called 'e-government') cannot be grasped by parliaments or by popularly elected bodies in territorial space (e.g. states)

2. – ICT applications for transfrontier transactions, from information exchange to cooperation between judicial and police authorities, while crossing jurisdiction exacerbate divergence and erode the quintessential equality of the citizen's access to justice and government.

3. - ICTs elude transparent 'control' by anyone other than those who (a) devised their programmes and (b) those who use them (for legitimate or criminal purposes).

The third point applies to ICTs regardless of whether they are used for 'domestic' or 'security' purposes. The fiascos over the ease with which hackers decoded the new generation of digital biometric passports, or worse still discovered – as in the Belgian case - that encryption was missing, suggests that makers of ICT programmes and systems

competing for market share prioritise vested commercial interests over data protection and system security.

ICTs facilitate the social construction of non-territorially defined public spheres by individuals communicating with each other over common interests, whether trivial or political. It is difficult to insert into this individualised scenario the concept of transparent and legitimate sources of authority that can be held accountable to territorially based institutions. Instead, there is a legitimate concern with ensuring that (i) territorial governments do not use new ICTs to enhance secrecy over the conduct of public affairs (paid for by the public), and (ii) do not apply ICTs in unknown ways that compromise individual privacy and liberty.

Little attention has been paid to the desirability or ability of parliaments – as the elected voice of the people – to ensure that ICT use by public agencies (let alone elusive private or commercial interests) are 'controlled' and answerable to parliament. Instead of an over-arching principle and genuine political control and accountability, there has been piecemeal legislation on data protection, spam, retention of internet data, data mining, fraud and misuse. Insecurity has been transmitted in the name of security. Transparency and openness codes have been prescribed and periodically updated without sufficient attention being given to the e-administration of government which potentially denudes parliaments of real control and capacity to hold government accountable.

3. Implications for parliaments of i2015 : Digi-space, communication and the public sphere

Historically, the cause of openness in the European Community and EU institutions has run in parallel with the adoption of ICTs. The problem is that the question of accountability has taken two separate paths: (i) the constitutionalisation of greater legislative power for the European Parliament; and (ii) the advocacy of codes of practice in respect of data management by ICT suppliers and creators. Common to both has been concern with 'communication' by enhancing (and accelerating) the exchange of information procedurally and openly by the legislative arms of the EU. When openness and transparency norms encounter ICTs, a new dimension of confusion appears and the obsolescence of traditional means of preventing the abuse of power is highlighted. The question is then, what would be an appropriate role for parliaments?

To address this question, it will be useful to reflect briefly on communication in the public sphere. Traditionally parliaments are expected to perform the Grand Forum role in democratic polities. As channels of communication, of information exchange, they are framing issues, shaping debate and influencing, albeit it to a limited degree, the content of draft legislation. The ability to do so in the area of freedom, security and justice is constrained constitutionally. It is also limited by the exemptions to rules on transparency and access to official documents, as well as by national practices on exceptions (notably regarding state security, secrecy and related issues) and national and

supranational discrepancies arising from differential application of the principles of access obligations enshrined in legislative commitments to openness and transparency within sub-committees, ad hoc or expert committees of national parliaments and, notably, in comitology[6] in the EU (Vos et al).

Exemptions are widespread and actual openness depends often on the discretion of officials as well as on the letter of the law. Moreover, the emphasis on improving access to documents has resulted in efforts to define what is meant by 'document'. This in turn has expanded the scope of document from the traditional paper 'document' to include digi-documents, microfiche etc. The problem with the latter is one of durability: paper survives better. Moreover, there is the question of definition: digi-documents require a greater degree of precision and uniformity in defining data fields, data content and terminology, if the intention is to permit automated data exchange. Data exchange and information exchange are not the same thing as intelligence exchange.

Whereas the granting of access to official documents both at EU level, notably by the Council, and at the level of member states continues to be uneven, public access is improving. At the same time, actual access may depend on the discretion invested in civil servants, and the completeness and the timing of the release of official information typically skewed to reflect and suit given institutions' interests. This operates at various levels and traditionally impedes the effectiveness of scrutiny of executive proposals by parliaments (notably in the European Community until first the cooperation procedure and then co-decision were entrenched). It also has a public face in the form of an element of political communication dubbed 'spin'.

Political communication in the public arena has traditionally been mediated by parliaments and the media, with MPs and governments being seen and depicted as the ultimate locus of authority and legitimacy. Parliaments, through ideologically inspired elected representatives of the people, have performed the role of discussion partner. Their target has normally and primarily been citizens in territorial bounded space. The problem is that this role has slipped and is being eroded by new media and means of communication and governance (Collins). Why?

The paradox of modern political communication matches that of the proximity paradox of bringing the EU closer to the citizen (Lodge, 2005). ICT tools expedite the transmission of information to the individual directly on a self-selecting, immediate and personalised basis. ICTs facilitate the social construction of non-territorially defined public sphere by citizens communicating with each other over common interests, whether trivial or political. Without going into the debate on the framing of the public sphere, it is important to note that alongside political communication by traditional voices and interest aggregators (parties, MPs and governments) ICTs have helped individuals establish an 'alternative' public sphere. The latter is shaped by self-interested information providers in a non-territorially bounded cyber-space

[6] Comitology: committees have delegated tasks (mainly from the Commission) in respect of the adoption of measures to implement legislative tasks.

devoid of authority and, crucially, eluding public accountability. Irresponsible and criminal activity (such as by traffickers, pornography merchants and paedophiles) can be tracked, traced and surveilled, using ICTs, and territorial forces used to capture the purveyors according to territorial rules and practices. The public generally accepts this application in ICTs to combat crime as necessary, legitimate, desirable and defensible. But insufficient distinctions are drawn between this use of ICTs and those associated with other domains from surveillance (giving rise to suspicion of Big Brother societies) to commerce, on-line transactions, blogging and leisure. A cursory look at spoofing and phishing for financial gain by criminals highlights the problem of policing and mediation in cyber space.

The proliferation of information and lack of means of verifying the dependability, accuracy, legitimacy, factual objectivity and authenticity of information placed on the web (such as that created in wikis) means that it is not immediately clear, least of all to the unsuspecting citizen, what the source or legitimacy of the source is. While there has been greater publicity about the dangers of online fraud, bogus banking sites and insider fraud in respect of commerce, a 'health warning' as to the validity of political or judicial sites is rare. Instead, there is publicity over corruption and public authority failures to ensure the security of personal information lodged in data banks accessible by other public authorities or agencies.[7] This leads to (i) falling public trust in government, and (ii) a serious shift in perceptions as to the loci of responsibility and accountability. Combined with seeming securitisation of an every increasing number of domestic policy issues, this obscures the issue at the heart of the dilemma of modern government: the tools chosen for communicating information.

4. E-Government: the unintended corrosive impact on parliamentary accountability?

In the absence of political authority and of an authoritative mediator, can political authority in cyberspace be established without a critical understanding and knowledge of the nature and practice of legitimate authority? Can the use of ICTs both by governments and individuals liberate citizens to engage in a public political sphere and protect their security? Or is the unintended consequence of ICT tools for private and public purposes the end of the principles and practice of political accountability? Do ICT tools inexorably rob parliaments and government of authority, and erase public consent over the ultimate locus of legitimate political authority?

The impact of ICTs on the public administration of government highlights an unforeseen and uncharted dilemma of ensuring public accountability for policy outcomes. ICTs change the way in which government is administered.

[7] Particular concerns arose during successive EU enlargements and methods for expediting new states' participation in police and judicial agencies through, for instance, the 2005 Act of accession of Bulgaria and Romania. It introduced a simplified system which by virtue of the Act of Accession Bulgaria and Romania accede to the conventions (and protocols) concluded by the Member States on the basis of Art. 34 TEU (previously Art. K.3 TEU) or Art. 293 EC. See the Convention of 26 May 1997, drawn up on the basis of Article K.3(2)(c) of the Treaty on European Union, on the fight against corruption involving officials of the European Communities or officials of Member States of the European Union. See COM/2007/0218 final-CNS 2007/0072.

They dissolve administrative boundaries. They transform the nature and practice of democracy, and the relationship between the state and the citizen. They require a re-assessment of political claims-making regarding democratic norms, and the principles of transparency and openness, the custodians of which are national parliaments in democratic polities in general, and the European Parliament in the EU in particular.

If e-government erodes administrative boundaries what is the consequence for codes of transparency and openness and ministers' accountability to parliament? Is transparency rapidly becoming no more than an ideal or a slogan? Do ICTs erode it in practice as administrative boundaries disintegrate?: The answer is either zero sum – most exceptions resulting for security leakage, or more openness and universalised co-decision. It is not clear that the adoption of more and more codes of general exemption deliver the goal that they are claimed to. It is, however, obvious that some papers cannot be disclosed for good tactical and strategic reasons (e.g. negotiating position papers; those likely to harm relations with other states; high level policy briefings). It is equally important to recognise that the disclosure of participants or those privy to some discussions is not the same thing as openness and public accountability. However, disclosure of lists of who's an outside expert whom a committee may consult; departmental participation; and critically disclosure of ICT providers (the vested interests) offers a modicum of transparency. From this, there is some chance of tracking activity on a post hoc basis, at least to determine possible sources and channels of influence, whether undue or legitimate.

Observance of codes and practices of transparency and openness are supposed to lend legitimacy to decision-makers. ICTs for the purpose of e-government provide virtual openness and visibility but no means of exacting political accountability: e-democracy is a misnomer. E-Voting is but one element of democratic practice. In the specific arena of freedom, security and justice, and as administrative boundaries merge, two contradictory obligations collide: transparency and the principle of availability. The first is a prerequisite of parliamentary accountability and democratic legitimacy; the second a prerequisite of enhancing crossborder and police cooperation in respect of 'criminal' matters, however differentially and expansively that term is defined. The first can be antithetical in practice to operational goal attainment and the effective apprehension of suspects; and the second vulnerable to known risks accruing from dependence on automated information exchange and, potentially, universalised inter-operability. All may seriously compromise optimal goal attainment (EP, LIBE 2007). The risks include: system incompatibilities; system obsolescence; insider attack; fraud; hostile intrusion; incomplete data; data storage and degradation; data mining; imperfect data management codes of conduct for managing data inputters and data transfer; authentication; verification; legal codes; data ownership; data protection and privacy and laws on use, misuse, re-use, re-sale and reconfiguration misuse of computerised information.

Automated data exchange moreover side-steps the human face of information exchange and the mutual trust and security networks built up by human contact. ICTs do not replicate them, for the time being. Claims that information

can be securely exchanged among mutually trusted agencies on bilateral or multilateral bases may be true but not necessarily universally so, and the underlying ICT systems may not be universally compatible or transferable from one policy arena to another, even if an increasing number of governments opts for open-source software applications.

5. Privatising accountability versus ICTs amenable to national parliamentary control

The problem for governments and parliaments regarding the responsibility for public policy and data use for public policy purposes lies with the way in which the roll out of ICTs has occurred. In practice, by relying on discretionary codes of practice for managing the input, use and storage of personal data, governments have allowed a form of privatised control over public policy to occur. Individual privacy has been compromised by the behaviour of private and government agencies (as in the well documented cases of data loss and theft). Parliaments appear to have suffered a loss in their authority as a result. This means that if they are to be effective in exercising their grand forum and voice of the people scrutiny and control roles, they have to be both more vigilant, more expert and more adept at exchanging and use ICTs for their own information exchange purposes. Few are sufficiently able to do this. In addition, they need to exploit the expertise of the data protection supervisors and work with the European Data Protection Supervisor, ombudsmen and especially the EP's LIBE committee to be in a position to be able to question and hold the EU Commission and both national governments singly and collectively (in the Council of Ministers) to account. Post hoc reliance on legal redress is a necessary but not a sufficient condition of ensuring openness, legitimacy and democratic accountability. Without those, individual and collective liberty and security are at risk.

Evidence grows of rising breaches of data privacy, weak public accountability by public bodies using ICTs for transmitting information and personal data for public purposes, and a raft of problems over the inadequacies of the security architectures in place. For example, the European Commission launched proceedings against Germany, Austria and the United Kingdom for breaches of Community data protection law. In April 2007, France's data protection authority, the CNIL (Commission Nationale de l'informatique et des Libertés) fined the US-based Tyco Healthcare France corporation 30,000 Euros for non-cooperation and for providing CNIL with erroneous information. In March 2007, the Garante, Italy's data protection authority, issued a guidance paper to assist employers to overcome some of the hurdles and to allow monitoring in a way that satisfies the requirements of the EU Data Protection Directive as implemented in Italy. The paper contained a legally binding interpretation of the statutory requirements for monitoring in the workplace.[8] In Britain, the government was repeatedly embarrassed by data losses arising from sloppy handling.

This is just the tip of an iceberg. The problems of ensuring parliamentary

[8] Privacy Laws and Business Newsletter, May 2007.

control at any level, whether local, regional, national or European, are extremely difficult in a situation where technical and technocratic 'expertise' dominate. Prioritising efficiency gains and cost-cutting is risky to states and individuals, but lucrative to ICT vendors. Parliamentary accountability mechanisms have not caught up with contemporary realities and civil servants are often ill-placed to assess the risks. Over simplistic assumptions and claims are made; over-optimistic goals set (as with the elaboration and realisation of a common consular space, cooperative offices; and biometric visa processing in localised offices). Avoidable breaches of data processing security ensue. The question of who is responsible and accountable in these mixed private public partnerships cannot go on being dealt with on an ad hoc basis when 'scandals' occur without compromising still further public trust in government and parliaments. Trust is at the heart of legitimacy.

Conclusion

The roll-out of ICTs for public service efficiency gains and citizen convenience gains (ignoring the digi-divide and the socially excluded) is accompanied by disingenuous, sometimes naïve assumptions as to their allegedly 'democratic' character, and by credulous but deceptive political claims-making as to their contribution to enhancing transparency and openness. Yet, if the latter are not to be robbed of genuine import and meaning, accountability to parliament must be realised. Accordingly, the European Parliament should adopt a more critical approach to transparency and demand genuine transparency regarding the ICT tools used for public policy purposes. Its' lever lies in the Reform Treaty and pillar I (asylum and immigration); pillar III (police and judicial cooperation); the Hague Programme; and other sectoral policies. It should begin by embedding and mainstreaming ICT risk assessment and requirements for all policies subject to EU competence, including soft law instruments. It should review 'discretionary' power to exempt issues from transparency and openness and make them uniform, including issues on declassifying documents (such as 50 year secrecy rules, and discretion to define any matter secret). Data Protection supervisors should be critical and forward-looking, pro-active and co-opted by the EP to alert governments to likely problems and empowered to look into data management procedures to ensure protection. The EP and national parliaments should 'embarrass' governments over the improper use of data, powers to act against agencies who refuse to submit files for scrutiny claiming that they are subject to exceptions (and exemption from transparency and openness access rules). Obligatory reports to EU authorities should be detailed; those which are not sufficiently detailed and which fail to meet standards set by the EU Data Protection Advisor (EDPS) should entail penalties that immediately compromise the ability of the local agencies to conduct their business. For instance, if an agency does not comply with both data protection legislation and high uniform standards of data procedures, access to important data bases (e.g .Schengen II) should be barred.

In short, the EP has to take the initiative to ensure greater cooperation with national parliaments and do so before the next Euro-elections. Tangible results, close to the people, are likely to

have greater mobilisation potential and be of greater interest to the individual, than the prospect of MEPs electing the Commission President, interesting as that constitutional requirement may be in its own right. Declining public trust in the integrity of government and politics, the authoritativeness of the media and the trustworthiness of private and public bodies handling personal information, undermines the credibility of states' claims about how ICTs contribute to personal and collective liberty and security. The Council of the European Union recognised this in November 2008. But action should not stop at the Commission's forthcoming communication on future priorities in the fields of Liberty, Security and Justice in Europe which will prefigure the next long-term programme (2010-2014) and the fight against cybercrime. The EP must critically assess the Commission's evaluation of the implementation of Directive 2006/24/CE of the European Parliament and the Council of 15 March 2006, regarding data retention, and follow up the work of the Article 29 Committee[9] to ensure that the latest Council statements (Council 2008) are not eroded by the practical realities of ICT advances in domestic e-government and commercial activity. It must take insufficient steps to reassert democratic controls and accountability. Baking-in them into the design of e-government should be the norm.

REFERENCES

- Article 29 Data Protection Working Party (2007) *Opinion 4/2007 on the concept of personal data*. Brussels 01248/07/EN.WP136
- Balzacq, T. and Carrera, S.,(eds) (2006) *Security versus Freedom?* London: Ashgate
- Collins, R. (2008) 'Trust and Trusworthiness in the Fourth and Fifth Estates', *International Journal of Communication* 2 :61-86
- Council of the European Union, (2008) *Council Conclusions on a Concerted Work Strategy and Practical Measures to combat cyber-crime*. Brussels.
- Curtin, D. (2001) 'Emerging Institutional Parameters and Organised Difference in the European Union', in E.Vos, D.Hanf, B de Witte (2001), *The Many Faces of Differentiation in EU Law*, Antwerp, Intersentia
- Delhey, J. (2007) 'Do Enlargements make the EU less cohesive? An Analysis of Trust between EU Nationalities' *Journal of Common Market Studies*, 45:2:253-79.
- European Commission (1979) COM(79 650 final. *Report on European society faced with the challenge of the new information technologies: a Community Response*

[9] Article 29 Data Protection Working Party was set up under Art 29 of Directive 95/46/EC as an independent advisory body on data protection and privacy. Its takes are outlined in Art 30 of Directive 95/46/EC and Art 15 of Directive 2002/58/EC. Secretariat is provided by the Commission JLS.

- European Data Protection Supervisor (2008), *Third Opinion on the Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters* OJ C139, 23/07/08
- European Parliament LIBE *Committee of the European Parliament on the Future of Europol, 10 April 2007. J. Lodge Information, Intelligence and Inter-operability : the principle of availability and the problem of biometricised security*. Evidence to the Public Hearing
- Herman, V & J. Lodge (1979), *The European Parliament*, London, Macmillan.
- House of Lords, (2007-8) European Union Committee, 29th report. HL Paper 183. *Europol: coordinating the fight against organised crime*
- Hoff, J., et.al. (eds) (2000) *Democratic Governance and New Technology*, London: Routledge
- Joerges, C., (1997) 'The impact of European integration on private law:reductionist perception, true conflicts and a new constitutional perspective. Private governance, democratic constitutionalism and supranational', *European Law Journal* 3: 378-406.
- Lodge, J., (2005) eJustice, Security and Biometrics: the EU's Proximity Paradox, *European Journal of Crime, Criminal Law and Criminal Justice*, 13/4, pp. 533-564
- Lodge, J., (Ed) (2007) *Are you who you say you are? The EU and Biometric borders*. Wolf: Nijmegen
- Nuffield Council on Biomethics (2007), *Forensic use of bioinformation: ethical issues*. Consultation Paper, London.
- Tchorbadjiyska, A., (2007) 'Bulgarian Experience with Visa Policy in the Accession Process.' *Regio* 10: 88-105
- Vos, E. D. Hanf, B. de Witte (2001), *The Many Faces of Differentiation in EU Law*, Antwerp, Intersentia