Freedom, security and justice: the thin end of the wedge for biometrics?

Juliet Lodge
Jean Monnet European Centre of Excellence, Institution of Communication Studies, University of Leeds, United Kingdom

Summary. This paper examines an area of EU policy where the application of information and communication tecnology (ICT) poses acutely difficult problems for policymakers: freedom, security and justice. It focuses on the absence of an ethical debate about the adoption of ICT-based instruments in this area. It highlights the implausibility of simply adopting codes of ethical practice from the health sector to close the public trust deficit. It argues that health and justice professionals need to cooperate in order to create a code of ethical e-governance fit for an e-governance age.

Key words: security, ethics, e-governance, biometrics, democracy.

Riassunto *(Libertà, sicurezza e giustizia: un passo avanti verso la biometria)*. Questo articolo esamina un'area delle politiche europee dove l'applicazione di tecnologie informatiche pone importanti e difficili problemi ai politici: libertà, sicurezza e giustizia. L'articolo fa il punto sull'assenza di dibattito attorno alle implicazioni etiche sollevate dall'adozione di strumenti informatici in questa area. Sottolinea come sia improponibile la semplice adozione di codici etici dal settore sanitario per rimediare al deficit di fiducia da parte dei cittadini. Sostiene che i professionisti della sanità e della giustizia hanno la necessità di cooperare per creare un codice di *e-governance* adatto all'epoca dell'*e-governance*.

Parole chiave: sicurezza, etica, e-governance, biometria, democrazia.

INTRODUCTION

The European Union is committed to creating sustainable freedom, security and justice. In order to attain this ambitious goal, the EU envisages numerous programmes, measures and framework decisions to facilitate judicial cooperation. The e-Justice project has two elements. One focuses on ICT as a means to expedite and facilitate judicial cooperation. The other concerns the ethical issues raised by implementing core principles – such as proportionality, fitness for purpose, and availability – in the absence of sufficient democratic political accountability for e-governance.

This paper outlines some of the problems in the area covered by e-Justice: freedom, security and justice, an area of EU policy where the application of ICT poses acutely difficult problems for policymakers. It highlights the absence of an ethical debate about the adoption of ICT-based instruments in this area. It stresses the implausibility of simply adopting codes of ethical practice from the health sector to close the public trust deficit. It argues that health and justice professionals need to cooperate with others in order to create a code of ethical egovernance fit for an e-governance age.

E-JUSTICE

Under a f6p (sixth EU framework programme) called e-Justice work has proceeded to pilot and model cross frontier judicial cooperation facilitated by ICT in four core areas: rogatory letters, the European Arrest Warrant and euro-payments. This paper is not concerned with the content of the policies. Rather, it focuses on the ethical and democratic dilemmas raised by applying ICT to the process of prosecuting crime across different jurisdictions within the EU.

E-Justice provides a demonstration project of judicial cooperation in the areas where it should be possible to identify:

- technical feasibilities of authentication and access;
- make a preliminary identification of a *capabilities audit* of law enforcement authorities in using state of the art technologies and next generation technologies;
- identify costs of non-comparability in capacity of different Member States (financial, political, technical and training implications);
- identify appropriate level of access and authentication rights, *e.g.* is it possible to consider *ab initio* ways of regulating authentication and access in order to prevent the selling of data by either public authorities or private agencies that may have accessed data about individuals (*e.g.*, as in the US). Does this require examination of property rights?
- types of data needed to make judicial cooperation effective (as part of the effectiveness audit) *e.g.*, needs of the European Arrest Warrant; rogatory letters, etc.

Indirizzo per la corrispondenza (Address for correspondence): Juliet Lodge, Jean Monnet European Centre of Excellence, Institute of Communication Studies, University of Leeds, LS2 9JT, United Kingdom. E-mail: j.e.lodge@leeds.ac.uk.

E-Justice seeks to identify how e-judicial cooperation across frontiers is evolving with a view to identifying and accessing the nature and level of democratic accountability mechanisms and codes of procedure and regulation that could form the basis of a common "gold" standard for ethical use of ICT and biometrics across e-governance policy sectors. Its starting point is cross-frontier judicial cooperation in respect of organised crime because this is the most sensitive area to which governments and the EU Commission routinely allude in order to justify the introduction of biometric, digitised identity documents. The objectives are to help identify and formulate consistent, coherent ethical parameters for egovernance and responsibilities.

JUDICIAL COOPERATION: THE CHALLENGE

Judicial cooperation is seen as essential to combat international organised crime and terrorism, and to enable the EU to develop a common effective, fair and just asylum and immigration policy. The territorial scope of the EU and its Member States provide the starting point for this but the justice, freedom and security goals of pillar III are predicated on assumptions about the e-governance advantages of capitalising on technological innovation in non-territorial space. The European Council's overarching goal of facilitating information and data exchange among judicial, security and law enforcement authorities rests on the explicit assertion of a borderless area of e-judicial data exchange. The Brussels European Council of 4-5 November 2004 stated: "The mere fact that information crosses borders should no longer be relevant"[1]. This translates into the principle of availability whereby if information exists in one Member State, it should be made available to corresponding agencies in other Member States.

Realising a more secure and safer society within the borders of the EU is a common goal of the EU's member governments. The instruments chosen to facilitate this increasingly rely on the application of ever more controversial information and communication technologies (ICT), including "biometric identifiers". The problem for EU and member government decision makers is that the public neither trusts them nor those who employ them to safeguard the privacy and integrity of the individual. Thus, while these technologies potentially bring the EU – at least symbolically – ever closer to the citizen, they give rise to a paradox of proximity: the greater closeness they imply is defied by increasing public distancing from those issuing them: public distrust of governments increases as government agencies reach ever deeper into the personal space of the individual. As a result, a communication deficit arises that exacerbates the trust deficit in the EU at the very time when ICT are deployed with a view to convincing the public that their security and safety is paramount and being better protected by the ICT.

Suspicions remain that: e-judicial cooperation instruments and agencies will escape appropriate democratic controls; the principle of "availability" will enable agencies to elude appropriate oversight; and that as a result "unethical" procedures and practices will arise that will erode and compromise individual privacy. Democratic controls are not believed to keep pace with technological advances which citizens see as unnecessarily intrusive, expensive, and open to fraud and subject to inadequate ethical oversight procedures.

The collection, storage, automatic transmission, ownership and particularly the use and application of biometric information is accelerating in the absence of proportionate, consistent, ethical or democratically legitimated legal regulations or appropriate codes or procedures regarding virtual identity, privacy transfer and related rights. This situation poses risks to civil society, democratic governance, the integrity of law and legal procedures, competitiveness and security, and compromises public trust in the EU. It endangers some of the core objectives of the EU (such as solidarity) and the core legal principles underlying the EU (including those that can be loosely grouped under the headings of equality and non-discrimination; a level-playing field for the Single Market in all its dimensions; e-judicial cooperation, security, law and order).

E-JUDICIAL COOPERATION *VERSUS* FREEDOM, DEMOCRACY AND JUSTICE

The EU implicit assumption is that e-judicial cooperation has minimal costs over and above the hardware requirements. However, it will be difficult to reconcile the requirements of liberty, freedom, democracy and justice with the operational needs and priorities of security. By taking just one aspect of e-judicial cooperation – information exchange – the tensions between the security imperative and the implications associated with the collation and exchange of personal and sometimes sensitive information across and within jurisdictions shows how problematic it is to balance security with ethical, democratic e-governance. From the point of view of the EU, its goal of an ever closer union is brought nearer by the one policy area that evokes the greatest public suspicion: internal security.

The use of ICT deploying biometric identifiers gives rise to fears about "Big Brother" and potentially exacerbates the public trust deficit in government broadly conceived. The reasons offered by government to justify the collection and storage of biometric data in inter-operable databases create suspicion as to the proportionality of the measures proposed to the goals to be attained. Government agencies are seen to have "unethical" goals and practices; policies and instruments are poorly ex-

plained, and the trust deficit widens. At EU level, the proposed use of e-government ICT based on the principle of availability to realise judicial cooperation raises particular concerns. The transfer of responsibility for data protection, moreover, from the Internal Market DG to that concerned with pillar three issues potentially threatens to create a conflict of interest within the Commission since the former is geared to openness (with all the attendant parliamentary controls) and the latter to different decisionmaking rules not subject to effective parliamentary input with or without the Constitution in place. The situation has been likened to putting a wolf in charge of sheep by Tony Bunyan of Statewatch in April 2005. If it is possible to identify appropriate and adequate ethical procedures to ensure accountability in this area, then lessons may be transferable to the interlocking and increasingly securitised areas of egovernance in general.

ETHICAL CONSIDERATIONS

The ethical problems raised by applying information and communication technologies to a range of policy sectors involving the transfer of sensitive personal data about individuals has so far been largely considered within the realm of civic and civil policy areas. These primarily concern matters relating to the swifter access to routine local services and routine administration of local government matters (such as applying for and processing online driving licences, local taxes, birth certificates etc.). These are issues where the individual citizen remains in the position of demandeur. Citizens rarely think much more about the data they make available to the relevant authorities for such purposes. More sensitive issues are raised in respect of the processing and sharing of individual health and social service records. Data privacy questions as well as the ethical questions of transparency, openness and accessibility of data to unknown people and unknown agencies have been articulated. In these cases, not only does the individual citizen very rapidly cease to be the demandeur and the subject voluntarily disclosing information, instead the citizen becomes a data subject whose information is manipulated by unknown agencies and people. High standards of ethical practice concerning data disclosure and data management are expected within organisations but these are not necessarily mandatory. Nor are they known to or approved by the individual citizen or their elected representatives in parliament. The problems this raises for all citizens in general and for the socially excluded, educationally disadvantaged, handicapped and marginalised ICT under-class are recognised but as yet insufficiently robustly addressed. They have been identified as problematic in terms of a human rights agenda. This is but part of the problem. Much remains to be done.

An inter-disciplinary exploration of how different policy sectors have addressed ethical issues – such as those that arise, for instance, in respect of stem cell research – may help us to identify common issues and build a common platform for ensuring that high ethical standards are obligatory and universally applied, maintained and enforced by agencies of e-governance in both the private and public sector.

INFORMATION AND COMMUNICATION TECNOLOGIES AND CRIME: RATIONALE

The application of information and communication technologies to cross-frontier judicial cooperation is considered to be an asset in tracking down and prosecuting crime. It is seen as adding value to efficient, effective administration in civil and criminal law, across frontiers and jurisdictions as well as within the territory of a given state in much the same, often non-critical way, that e-administration and e-governance are believed to have done. E-governance is believed to provide efficiency and effectiveness gains in the general administration of government. E-governance services are widely deployed: online payment of council taxes, registration of births and marriages, driving licence applications, social security and tax matters etc are common. The computer storage of health records. Is also becoming more wide-spread. The EU's e-health card scheme for the 2004 Greek Olympics was designed to facilitate swift checks on visiting individuals' entitlement to receive health care if necessary. However, e-health possibilities already outstrip the idea of an e-health card being used purely as a means of verifying individuals' entitlement to treatment. The creation of the verichip (inserted in an individual's body) as a means of authenticating and verifying an individual raises serious concerns about the technical incorruptibility of the data on the chip, as well as about the economic gains, and global commercial ambitions (sometimes dubbed biocolonialist inclinations) of the chip providers and data storers. More seriously, it raises concerns about the individual's right to privacy and ability to keep the implanted chip secure "for life". While it is argued that verichips would help accelerate the identification of corpses or body parts, the underlying ethical issues have been neglected. More importantly, the implications for the conduct of society and the presumed traditional relationship between the governed and the government have hardly been considered. Moreover, whereas these areas are usually seen to lie within the realm of civil life, fraud and criminal activities associated with the theft of identities (of all kinds, including biopiracy) evoke quite another scenario.

It is too readily assumed that e-governance is separate from "normal" political processes; that it is essential no more than a matter of presenting information on the web for apolitical purposes. As such, not only does it elude democratic accountability and controls but the latter are often not seen to be necessary. This fallacious assumption is especially challenged by the *implications and applications* of e-judicial cooperation.

e-judicial cooperation, as an arm and instrument of egovernance, when portrayed in terms of efficiency gains, occasions little concern. For example, online dispute resolution has its advocates and, although it is in its infancy, attention seems to focus on the quality of mediation online compared to face-to-face, much like in the case of e-learning. However, the instruments and practices, procedures and mechanisms for giving effect to e-judicial cooperation across frontiers – notably in criminal issues outside the asylum and immigration spheres under SIS and Eurodac, as well as in the difficult civil areas of family law – challenge our understanding of and trust in the robustness of our democratic accountability and openness mechanisms.

E-JUSTICE WITHOUT DEMOCRACY? THE ETHICS CHALLENGE

The introduction of mandatory biometric identifiers in passports has been opposed on the grounds of Big Brother. But this misses the point. Biometrics *per se* are not the problem. The central question has to be control over their use: who's controlling "big brother"?

If traditional territorial political controls in cyberspace are both inadequate and impossible to achieve, there is a vacuum in political accountability. This vacuum has not (yet) been filled by new cyber political accountability arrangements that are transparent, open tamper proof and subject to public surveillance, reform and overthrow. In cyberspace, the "masters" are the programmers and those transferring and accessing data on altogether nebulous, unclear, unexplained bases. The response to the publicly articulated concerns to this has been to examine management procedures internal to organisations. Ethics (loosely conceived) has become a vague argument deployed by those using or advocating the use of the technology to justify their adoption in the absence of genuine, traditional controls. Loosely defined and often voluntary ethical codes of practice not only vary across and within jurisdictions, private and public sectors, but they are insufficient and no substitute for democratic political controls. Are ethical requirements regarding the verification, authentication and robustness of procedures for accessing and holding, and the processes for transferring and exchanging e-data become a sufficient alternative? What do they mean? In the case of e-judicial cooperation, the "ethical issue" is presented as a test of proportionality and fitness-for-purpose. But proportionality and fitness for purpose are not necessarily adequate tests to ensure ethical practice. The internal security arena proves an illustration.

When the EU Commission and Council fell foul of the European Parliament over the exchange of passenger name data (PNR), their failure to respect EU democratic procedural requirements was highlighted. The question of the proportionality and fitness of the PNR measures themselves, though central to the EP's objections, were somewhat obscured by this. However, it is entirely proper that these procedures that flow from the constitution's structures are honoured: structures in the constitution provide and protect the collectivity – all citizens together, while individual rights protect the individual citizen. They are complementary and inseparable, mutually reinforcing and mutually dependant.

The "ethical" issues and tests, proportionality and fitness-for-purpose, are embedded in political constitutionally and territorially bounded concepts of democratic rights and responsibilities. This example highlights that. The problem is, however, that a further principle has been tied to these in the arena of e-judicial cooperation and the realisation of freedom, security and justice. That principle is the principle of availability. Its application is designed to: a) expedite data exchange; b) heighten efficient identification and prosecution of suspects; c) create consistency within and especially across jurisdictions by removing the need to first go through the procedures applicable within a particular jurisdiction which may result in significant delays and so undermine successful apprehension and prosecution of suspects and even compromise collective security. The principle of availability means that if data is available in one state that is potentially useful to another, it must be made freely available to the latter. At a technical level, this seems feasible. At a political level, it offends and compromises the requirements and sustainability of democratic practice and ideals of openness and public accountability.

It also potentially erodes individual fundamental rights and freedoms. This is nothing new. What is new, however, is the linkage between edata transfer for judicial purposes and the overarching role of the state and its overriding responsibility to maintain collective security. Without clearly addressing this and the ethical implications of e-governance, there is a danger that the profound shift in the relationship between the agents of the state and the citizen will be overlooked. There is more at state than the erosion of civil liberties. This is real but the focus on one aspect arising from opposition to the collection, storage and transfer of biometric e-data detracts from this.

The EU's Hague programme (2004) stressed expediting the means and adoption of the requisite technologies to facilitate cross-border cooperation and information exchange by law enforcement agencies in order to realise the overarching goal of sustainable freedom, security and justice. A stepped approach to this focuses on combating international organised crime and terrorism using instruments to track the movement of people across borders, including the collation of biometric data in inter-operable systems potentially linked to a central database. Central data storage raises numerous issues of trust and confidence in government and the practice of democracy. They relate to but go beyond: robust identity management systems to prevent system

abuse and identity theft, ambient intelligence systems, function creep, cost, accountability mechanisms and personal privacy. The Hague programme prioritises the enhancement of mutual trust, adoption of minimum substantive and procedural rules and methods of implementation. The European Parliament calls for a quality charter. The underlying assumptions, not yet probed, relate to the ethical underpinnings of the rules, principles and methods of implementation.

WHAT IS THE PROBLEM FOR THE EU?

The EU has a three dimensional horizontal and vertical challenge. The issues oncern:

1. nature of political control (institutional horizontal and vertical);
2. nature of technical/political processes (gold standards applied horizontally and vertically);
3. nature of differential regulatory frameworks at national, supranational and international levels.

There is a need to first create a shared vision for a cooperative approach, and create consensus on implementing effective instruments and mechanisms. This would lay the groundwork for creating a supranational structure complete with clear political accountability and control mechanisms. This shared vision cannot compensate for the lack of such political accountability at present. The risks are too great of doing nothing and allowing haphazard ambiguous, contradictory, partial and fragmented systems to develop.

That is not a sensible option for an organisation like the EU seeking to be a competitive international player, and it is certainly not one to be recommended to those wishing to develop an European solution or model to a universal problem which will otherwise be defined by other larger players who may not share the EU's commitment to democratic e-governance and protection of human rights. While s-takeholder forums might help to better identify players concerns and ambitions, the time lag between deliberation and action could be too long to allow the EU to develop an appropriate model. This needs to be complemented by independent, external interdisciplinary analysis of stakeholder goals and "solutions" to rendering function creep democratically accountable. Ethical practice in egovernance, and especially in the sensitive domaine of e-judicial cooperation must pave the way for bolder, integrated political steps if the EU is to remain on the playing board of e-governance in all its dimensions.

E-JUSTICE: THE CHALLENGING SEARCH FOR ETHICAL E-GOVERNANCE

The UK has some of the most comprehensive legislation on terrorism and data retention of all the Member States. The UK, Ireland, Sweden and France put forward a Draft Framework Decision on Data Retention which not only lacks the safeguards of the SIS mechanisms but is symptomatic of: a) function creep; b) ambiguity and imprecision in respect of the who, what, why and when of the proposed measures. The e-Justice Committee convened in the UK has been examining a series of questions relating to the need to ensure proportionality and consistency in any EU *and crucially national* legislation giving effect to ejudicial cooperation, including data retention. This requires discussion of the nature and purpose of accessing and retaining data on individuals. The starting point for the initial discussion was the JAI DG Consultation Document on Traffic Data Retention published on July 30 2004. It was produced by INFSODG Information Society (Dir B – Communication services: policy and regulation framework) and DG JHA Dir D (Internal Security and Criminal Justice).

Actual workflows within judicial processes have been modelled by e-Justice and an ICT-based deployment system has been developed that is as secure as any, and allows documents to be readily tracked and identified (but accessed only under strict verification and authentication) within and across jurisdictions. If e-Justice can show that the technology works and is secure, the problem that remains concerns the public trust deficit.

In general, publics across the EU do not trust the idea of interoperable data bases, central data storage and automatic information transmission because it implies a loss of ownership by the individual of the self and also because too much is unknown (and in criminal matters has to be unknowable – judicial and police authorities would argue, for operational reasons). Success depends on secrecy. The facelessness and advantages of e-administration where the individual as demandeur can opt out of the process at will becomes a distinct disadvantage in the context of e-judicial cooperation in both civil and criminal matters. Somewhat paradoxically therefore there is a need for a visible, human interface to be re-established in e-governance that is more than a cosmetic "voice" or façade. E-governance, no matter how sophisticated and universalised, cannot forever evade the democratic needs and requirements of modern society. The problem is that these are poorly articulated outside human rights discourse and ICT advances outstrip knowledge readily available to be voiced by politicians and publics alike.

Accordingly, there is a need for e-Justice ethics work to consider:

- existing practices (who has access, how is it authorised, how (*e.g.*, judicial orders?);
- actual needs (why and when);
- capabilities (technical feasibility *e.g.*, what systems are used; identification of absence of comparability and inter-operability; training needs of personnel; codes of practice);
- effectiveness audit (analysis of safeguards);
- elaboration of common rules, training and standards to facilitate a level playing field, guard against discrimination, arbitrary application, non-comparability, and risks of corruption.

Member States' laws on data retention, for example, are not comparable. There is evidence of disproportionality, function creep and a lack of clarity about what is technically feasible, as opposed to what is on the wish list of certain governments. The dual problems of authentication and access highlight a critical obstacle to the realisation of a common playing field in ejudicial cooperation, and across other e-governance arenas.

National rules remain paramount. If harmonisation and commonality are not yet possible, then a step towards that is offered by e-Justice in its models of tracking systems and making cross-country comparison simple to see, understand, track and operate.

This does not dispense with the need to identify the EU baseline legal framework on biometrics, and biometry in e-governance; provide an overview of ethical and legal issues related to biometrics (robust identity management, automatic authentication, data storage, transfer and inter-operability, and function creep); and describe legal and regulatory frameworks (where they exist) for different biometric technologies. Different tasks and goals may have different security requirements especially in the Member States; indicate how existing institutional frameworks need to be modified in order to a) secure civil society confidence in the proportionality and legitimacy of policy relating to the one issue that affects each individual and which potentially brings the EU closest than ever before to the citizen: biometrics; b) seek to identify a *parameter of sufficiency* and issues needing further regulation to create a balance between security and privacy and sustain proportionality and consistency across the member states; identify the ethical, legal and institutional challenges and risks to the EU arising from inadequate common rules on e-governance in general as the technological feasibilities of collating, selling and automatically exchanging biometric data exceed what is necessary for the transaction envisaged and escape democratic oversight, thereby posing significant legal risks; and to assess whether there is a need for EU level regulation and changes to the legal framework to complement existing practice in the member states, and if so what changes are needed and how they can be given effect. E-Justice begins this by providing a tool, and building block.

ETHICAL TOOLS

The Commission's commitment [2] to enhancing ethical and social debate and to integrating discussion platforms as a strategic element of research highlights the need for the ethical questions concerning the application of biotechnology to new fields of science. The implementation and application of such technologies, for example, by governments at all levels raises specific issues of ownership, intellectual and property rights which have been addressed in the relevant Directives awaiting complete implementation across the 25.

While life sciences have addressed the ethical issues (*e.g.*, in respect of GMOs and human embryo cloning), newer applications of science based biotechnology to other fields of governance of central importance to the EU, have not. In particular, the EU's commitment to the realisation of freedom, security and justice, and to sustainable and dependable security raises, in its operationalisation through the introduction of biometric identity cards, passports and databases (beyond those in Schengen, SIS-VIS and Eurodac) a number of ethical issues that are only beginning to be discussed.

Discussions within forums concerned with the promotion of judicial cooperation to help attain FSJ, suggest that there is wide variation among the Member States over attitudes to and practices relating to the storage and exchange among different administrative jurisdictions within national governments as well as across member states and further afield with private and public sectors. This presents the EU with a new range of problems concerning and going beyond not only intellectual and property law, legal practices, cyber law, human rights, privacy and data protection. The issue of digitised biometric smart cards and passports raises ethical issues about the ownership, authentication, possession, transfer, sale and accountability for any fraud or misuse of biometric data. There is a need to establish good practice and a gold standard in a new area of EU policymaking that applies science to the service of society, and notably to each individual's security.

Under-developed and inadequately exploited networking and information exchange potential among the various levels of governance within the EU in respect of judicial cooperation and sustainable security must be addressed. However, e-government and technology raise ethical issues which are central to understanding the potential for convincing the public of the necessity, desirability and appropriateness of ejudicial cooperation. Given that citizens will not have any choice but to accept e-governance, biometric identifiers etc. It is imperative that ethical and transparency concerns are seen to be addressed through appropriate institutional and instrumental means. Trust has still to be established and sustained.

There is an urgent need to discover what and whether there are proportionate measures that may be derived from a comparative assessment of the values, standards and ethical concerns that individual member states may have in respect of the application of biometrics to an ever widening sphere of e-governance. Mutual recognition of existing standards has already been ruled out in view of the wide discrepancies in respect for and trust in the law enforcement bodies in different Member States. It is important therefore to identify where there are convergent or common standards, values, and ethical concerns that could be used to try and discern a distinctive European standard. Without a European standard, ad hocism will prevail that will

compromise other EU goals – equal treatment, citizenship, non-discrimination and the charter of human rights – and will compromise the EU's ability to deliver its promises under the draft Constitution and remain an independent international player. If Europe is to deliver a European standard to the international community in an era of globalisation, it must accelerate its current work in this field.

Submitted on invitation.
Accepted on 4 October 2006.

References

1. Council of the European Union. *Point 2.2.1 European Council Presidency Conclusions, DOC 14292/04.* Brussels, 4-5 November 2004.
2. Commission of the European Communities. *Communication from the Commission to the European Parliament to the Council and to the European economic and social Committee life sciences and biotechnology COM(2003) 96 final – A strategy for Europe progress report and future orientations* (SEC (2003) 248); Brussels: CEC; 5.3.2003.