Globalization -
Strategies for Data Protection

Herbert Burkert

Data protection - by making use of epistemic communities, ensuring government support, profiting from reciprocal regulatory mechanisms and using international communication - has already applied successfully global strategies even before globalization became a general issue. However, current set backs for the role of data protection as well as the legitimacy crisis of globalization make it necessary to reflect on past strategies and to supplement them with new strategies to join forces with the private and the third sector, to keep a better track on technological developments internationally, and to improve training internationally. A renewed reflection on the basic role of data protection on the global scale should lead to joining forces with access to information institutions and lead to a renewed cross-cultural analysis of daily data protection practices.

I. Introduction

The title of this presentation is somewhat ambiguous; it poses at least two questions:

- Does globalization - as a set of strategies - provide examples from which data protection can learn to promote itself globally? And:
- Does data protection need specific strategies in the face of the challenges posed by globalization?

This presentation intends to answer both questions. Furthermore I will try to show that it is the answer to the first question which contains the essential elements for the answer to the second question.

II. Data Protection As A Global Concept

1. The Road to Success

The first question can be answered directly, but the answer will need an explanation: Data protection does not need to learn strategy from globalization. Data protection already applied many of the strategies which today are seen as strategies of globalization.

Do human rights need a strategies at all? As history shows they do need strategies and strategies have been used successfully. But before we look at data protection's strategies more closely, it has to be added that data protection had a privileged position which

largely contributed to its successful career so far: It had been the inherent logic of the issue itself that had helped its global expansion:

Data protection, if understood - in our context - as a legislative concept to meet challenges of information and communication technologies by minimizing the negative impact of these technologies on individuals and groups of individuals in order to maximize the beneficial impact of these technologies on society, had posed a simple choice. Adopted nationally it was limited to the geographic area of the competent legislator. The inherent logic of Information and communication technology, however, made distance, place and space irrelevant. Any responsible legislator would therefore have to use a device that at the same time would ensure that the logic of information and communication technology was captured in the interest of its citizens, while the regulatory approach respected the limits of legal competence.

Those were no theoretical and abstract considerations. One of the very first decisions of the first national data protection agency, the Swedish Data Inspection Board, had to deal with the export of personal data to a country with no data protection at that time, a decision which caused a broad international policy debate.

The answer was the "comparability" mechanism requiring - from national operators - and thus staying within the limits of national competence - to ensure that transfers took place only into countries with comparable protection. While this mechanism seemed to be aimed at bilateral rapprochement it carried a viral logic just as the technology itself: To maximize the benefits from information and communication technology the comparability mechanism had to work internationally. And so comparability made its international career

- as the *substantial observance clause* of Guideline no. 17 of the Organisation for Economic Co-operation and Development's Council Recommendation Concerning Guide-Lines Governing the Protection of Privacy and Transborder Flows of Personal Data of 1980[1];
- as the *equivalency clause* of Art. 12 Sec. 3a of the Council of Europe Convention of Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data of 1981[2],
- and - not without some reluctance - some fifteen years later as the *adequacy clause* of Art. 25 sec.1 of the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.[3]

---

1 Adopted by the Council 23 September 1980; see: http://www.datenschutz-berlin.de/gesetze/internat/ben.htm. - All links in this paper have last been verified on July 20, 2005. All links point to sources in English unless stated otherwise.

2 Council of Europe, European Treaty Series No. 108 signed January 28, 1981 - http://www.datenschutz-berlin.de/recht/eu/eurat/dskon_en.htm.

3 Official Journal of the European Communities of 23 November 1995 No L. 281 p. 31.

In the meanwhile data protection had received global recognition with the United Nations Guidelines Concerning Computerized Personal Data Files which were adopted by the General Assembly on 14 December 1990 and which transported Art.17 of the International Covenant on Civil and Political Rights (ICCPR)[4] into the present times.

We know that this did not imply that now every UN member state has fully operational data protection legislation in place or is even obliged to have such legislation. Nor does it mean that data protection and privacy are in the direct focus of the international community today. The (draft) resolutions of the 60th Session of the Commission of Human Rights of 2004[5] for example do not contain the word "privacy." The Human Rights Commission's NGO counterpart, Human Rights Watch, in its 2005 annual report mentions privacy, autonomy and dignity mainly in the context of sexual self-determination..[6] Other references in that report are about examples misusing privacy legislation to reduce the freedom of the press.[7]

Data protection is not the foremost issue of current international attention. This is a statement of fact and not of regret about not seeing one's own pet subject receiving that attention it would deserve. There is, however, still a problem here, and we will have to come back to it later. What is needed now is a brief look at the strategies applied.

2. Strategies applied

We may safely state - in the light of what apparently has been achieved - that within a relatively short time span, short at least for international law developments, data protection has reached the status of a universally accepted concept, even if it still falls short of a universally enforceable right.

Together with the viral logic already described it was a set of strategies, some of them chosen deliberately, some of them finding their way almost behind the back of the actors that helped to make data protection's international career, and finally, of course, there had been these windows of opportunity any strategy needs for its success.

In my view, at least four strategic elements are worth being mentioned here expressly:

- the use of epistemic communities,
- the use of government support,
- the use of the reciprocal adjustment technique,
- and the use of webs of communication.

---

4 International Covenant on Civil and Political Rights (ICCPR), G.A. res. 2200A (XXI), 21 U.N. GAOR Supp. (No. 16) at 52, U.N. Doc. A/6316 (1966), 999 U.N.T.S. 171, entered into force Mar. 23, 1976.

5 See: http://www.unhchr.ch/html/menu2/2/60chr/draftreport.htm.

6 Long, Scott: Anatomy of a Backlash: Sexuality and the “Cultural” War on Human Rights. In: Human Rights Watch: Annual Report 2005, pp.70ff. - http://hrw.org/wr2k5/wr2005.pdf.

7 Human Rights Watch: Annual Report 2005 p. 178 and p.201.

a) Epistemic communities

Epistemic communities are - in the words of Braithwaite and Drahos[8] - "loose collections of knowledge-based actors who share certain attitudes and values and substantive knowledge, as well as ways of thinking about how to use that knowledge".

At a time when the concept of privacy was present in scholarly discussions but was still lacking a conceptual and practical concept to be transformed into a workable regulatory concept it was this - from the beginning international - group of people rather than government experts and the usual rule makers who discussed ways and means to make the concept a reality. You are familiar with the names now inscribed in data protection's hall of fame. Their names appeared and re-appeared whenever a national government or international institutions were discussing data protection. In their testimonies they could mutually reinforce their arguments, refer to each other's authority and succeeded in establishing an international state of the art for data protection regulation.[9]

b) The involvement of governments

These groups would have remained influential but certainly less successful had they not ensured the support of governments.

The history of international human rights has shown that two main factors have largely contributed to the international establishment of human rights: First of all - and most unfortunately so - a collectively shared traumatic experience - and secondly the determined support of at least some governments with an international standing.

In my personal view four countries had been essential in showing that the concepts of those epistemic communities could be put into legislative practice by taking the lead in their respective environments; and to some of them that collective traumatic experience played an essential role as well:

- Germany, nonetheless because of its traumatic experiences with personal information in the hands of a ruthless government, by implementing the first data protection law ever in the State of Hesse;
- Sweden, being painfully aware at that time of the danger to the integrity of its national infrastructure as a neutral country in a divided world by establishing the first national data protection law;
- France, with the traumatic experience of German occupation, and with its will to set an example in its tradition of human rights;

---

8 Braithwaite, John; Drahos, Peter; (2000). Global Business Regulation. Cambridge University Press Cambridge 2000, p. 501.

9 See e.g. the descriptions of these processes in Flaherty, D.H.; (1989). Protecting Privacy in Surveillance Societies. Chapel Hill. London; Bennett, Colin J.; (1992). Regulating Privacy. Cornell University Press: Ithaca, London; Burkert, Herbert; (2000). Privacy - Data Protection - A German/European Perspective. In: Engel, Christoph; Keller, Kenneth H. (eds.): Governance of Global Networks in the Light of Differing Local Values. Nomos: Baden-Baden, pp. 43-70.

- and last but not least the United States of America a country from which most of the literature guiding the epistemic community originated, were active citizen interest groups were at work and which was still the second country with a national data protection law even if limited to the public sector.

In my retrospective analysis not all of these countries and those following later had purely altruistic motives compensating historical experiences. At that time in governments felt that the introduction process of the new technologies had to be smoothed in order to accommodate fears and suspicions and bridge a legitimacy gap as to the impact of these technologies. Moreover, on the international level it was realized that privacy might well turn out as an additional bargaining instrument in international discussions -although not as crudely as it had been suggested at that time when making reference to data protection as a non-tariff trade barrier. And indeed on the level of international trade law the WTO agreements took due notice of the importance of data protection by granting data protection the status of a "General Exception".[10]

c) The reciprocal adjustment technique

The reciprocal adjustment technique[11] is, of course, the mechanism which transposes the inherent logic of information and communication technology which I had mentioned above into legislative practice. Particularly in network economies it is sufficient that one country goes ahead - provided it is sufficiently important - to trigger off a chain reaction of mutual adjustments. The "sender country" principle of EU-.law is such a mechanism providing that compliance in one country assures acceptance in other countries. While these mechanism might lead to a race to the regulatory bottom regional regulatory systems like e.g. the European Union have taken care - and expressly so in the area of data protection - that standards are being kept which are not minimum standards.

d) Webs of communication

Human rights, too, and with them privacy and data protection need communication strategies. Data protection agencies have been fully aware of this necessity from the beginnings of their operations, a necessity which goes far beyond the reporting requirements imposed upon them by national legislation. In making ample use of the technology they had been installed to oversee, they had been able to not only reach out to their national constituencies. More so they soon became aware that these reports

---

10 Article XIV of the General Agreement on Trade in Services (GATS) at (ii). In detail: Perez Asinar, María Verónica: The WTO and the Protection of Personal Data. Do EU Measures Fall within GATS Exception? Which Future for Data Protection within the WTO e-commerce Context? - 18th BILETA Conference: Controlling Information in the Online Environment April, 2003 QMW, London - http://www.bileta.ac.uk/Document%20Library/1/The%20WTO%20and%20the%20Protection%20of%20Personal%20Data.%20Do%20EU%20Measures%20Fall%20within%20GATS%20Exception.pdf

11 See Braithwaite, John; Drahos, Peter; (2000), pp. 20ff., 543ff.

were read and compared internationally, by their counterparts as well as by a critical public, which also increasingly exchanged its views internationally.

Other means of communication like conferences of this kind, together with national, regional and issue oriented conferences not only helped to maintain public attention but also contributed to create something of an international epistemic community among data protection officers bridging the different cultural environments that formed everyday practices.

And finally, these communication means have increasingly been put to use as an effective platform for dialogue with non-governmental organizations, public interest groups and the international private sector.

e) A remark on windows of opportunity

In spite of all these techniques windows of opportunity were needed to ensure data protection's standing of today. Unfortunately windows of opportunity are usually only realized once they have been passed or when crashing against them because they have been closed. But it is useful to remember for any strategic exercise that such historical opportunities are needed.

3. Conclusion

Looking at today's endeavors in regulating globalization we encounter many of these strategies again and again, in the global environmental debate, in the global regulation of international property rights. While those striving for data protection may not have invented these strategies they at least have made good use of them.

III. At A Turning Point?

So all is well and we move from annual conference to annual conference with more and more participating countries until data protection has finally captured the globe?

Rather not, I fear. There is doubt, and there is uneasiness. We have started to view anything which carries the qualifiers "global" or "universal" with some doubt and premonition. Not that we question the global reach of information and communication technology, or that we neglect the phenomena of economic and cultural globalization, but we have started to question the intentions and forces behind these developments, we are skeptical about the inevitability of all their consequences, we worry about the desirability of all of their effects, we start to require balancing strategies if not outright counterstrategies, and we start to see the "local" in a new and brighter light. These tendencies in themselves have almost reached a global dimension.

Data protection which, as a principle, may have been uncontested as long as the exemptions were available at short reach is increasingly paying for the consequences of systematically addressing asymmetries in information distribution as issues of power

distribution between consumers and providers of goods and services, between employers and employees, between citizens and governments. The burden of argumentation once upon those who claimed exemptions from the data protection principles seems to be slowly shifting to data protection which is asked to prove that it is a functional and cost efficient human right. At times it is but a constitutional court - if available - which as a last resort tries to mend what willing parliaments had been ready to sacrifice and of course always for a good reason. Exemptions apply here as well, of course, as the recent European debate on data retention obligations has shown, although the final outcome of this debate is far from certain.

It is one of the characteristics of information and communication technology that it opens the asymmetry trap also common to other "big" technologies : Increasing dependence on information and communication technology only needs small destructive resources to create catastrophic effects. Since risk management efforts will consequently always need resources which are disproportional to the risk causing resources proportionality becomes an endangered specie and with it data protection.

This is not to suggest that there have not been in our societies, on the national, regional and international level powerful and unequivocal statements for data protection, as e.g. the decision of the Strasbourg Court in the case of Klass and Others vs. Germany or the famous German Constitutional Court case on the German census. But the times seem to be changing.

From my own experiences here in Geneva two months ago as a session chair at one of the topic conferences for the second part of the World Summit on the Information Society I have learnt how - at such an occasion and opportunity - in spite of many balancing contributions and efforts including those of the organizers data protection is in danger of being marginalized as just one hyphen in a list of considerations which all succumb to security.

This simultaneous set back for globalization *and* data protection comes at a time when it becomes more and more obvious what - if I remember correctly - the French Data Protection Act had expressed first and more than 25 years ago, that data protection is not just about accommodating privacy in an information and communication technology environment but that data protection is directly addressing this technology to keep it embedded in the political and legal responsibility of society as the suitable environment of all human and civil rights and the due democratic process by proclaiming :

> "L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques."[12]

---

[12] Article 1 Loi n° 78-17 du 6 Janvier 1978 relative à l'informatique, aux fichiers et aux libertés (Journal officiel du 7 janvier 1978 et rectificatif au J.O. du 25 janvier 1978) maintained in the latest version of the law (Loi n° 2004-801 du 6 août 2004 -(Journal officiel du 7 août 2004).

While this may just be one article of one particular data protection law we have come to learn that this conception has a universal reach with the universal spread of information and communication technology, and that in the interest of the universal future of all human rights data protection has to answer to its international calling and accomplish its global task.

IV. Carrying On A Global Task For A Universal Right : Future Strategies For Data Protection

And this brings us to the answer of the second question: Yes, data protection needs strategies to react to these changes, and in doing so data protection will have to re-examine its old strategies, and supplement them with additional support strategies.

1. Re-examining old strategies

a) Epistemic communities

In re-examining its old strategies data protection should and will still rely on epistemic communities, even if they have changed their face: They have become more diverse, larger and more complex and they have become more specialized in their dealings, as the development of the well known International Working Group on Data Protection in Telecommunications bears witness. Non-governmental organizations and citizen interest groups have increasingly developed independent expert knowledge and established networks which start to link with such communities. These networks of knowledge is increasingly used on the international level and data protection agencies should make sure to be part of such networks.

b) The involvement of governments

While at the beginning of data protection proliferation it had been necessary to secure the support of at least some national governments to start creating reciprocity effects which eventually inspired international organizations to provide for an appropriate common structure, now the emphasis has shifted even more to international organizations.

Even if many of them still operate in parallel, at times even in a competitive atmosphere, it is obvious - particularly since these organizations have become more inclusive as regards non-governmental organizations - that they now act as fora of global attention and attraction.

This new importance of international fora - also affects data protection as recently reflected in the discussions on Internet Governance and the already mentioned World Summit on the Information Society.

Any involvement of international organizations but also of the now included non-governmental organizations in data protection issues would certainly gain more international credibility if these organizations would more expressly commit themselves to data protection in their own organizations.

Furthermore, and particularly in the light of these shifts I have been referring to international organizations might want to remain more consistent in view of the commitments they have previously made to data protection.

In this context e.g. it is not without difficulty that I seek to understand why the Council of Europe's Cybercrime Convention[13] has not made it an explicit and formal prerequisite to become a party to the 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data before a state can become a signatory of the Cybercrime Convention.

The Cybercrime Convention has so far reaching consequences for - inter alia - data protection rights, and emphasizes that it is "mindful of the need to ensure a proper balance between the interests of law enforcement and respect for fundamental human rights as enshrined in the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms (...) which reaffirm the right of everyone to hold opinions without interference, as well as the right to freedom of expression, including the freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, and the rights concerning the respect for privacy" and "mindful also of the right to the protection of personal data, as conferred, for example, by the 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data."

Its proportionality and with it its legitimacy rests on the fully operational environment the Convention for the Protection of Human Rights and Fundamental Freedoms is providing, in particular, the direct rights to complain for citizens.

Still the Cybercrime Convention is open to non-member states, even to those non-member states who have not contributed to the drafting[14], although non-member states cannot become states of the Convention for the Protection of Human Rights and Fundamental Freedoms. So at least what could have been expected was to require adherence to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data which is open to non-member states. The only obligations that now rest upon such states are those references to the - non-enforceable - international instruments listed in Art. 15 of the Cybercrime Convention.[15]

---

13 European Treaty Series - No. 185 Convention on Cybercrime.

14 Art. 36 sec.1 and 37 sec.1 of the Cybercrime Convention.

15 See also e.g. International Working Group on Data Protection in Telecommunications Common Position on data protection aspects in the Draft Convention on cyber-crime of the Council of Europe adopted at the 28th meeting of the Working Group on 13./14. September 2000 in Berlin at http://www.datenschutz-berlin.de/doc/int/iwgdpt/cy_en.htm.

Such a treaty policy - in my view - is not an appropriate way to promote data protection in an international environment.[16]

One has to go - I believe - even one step further in the interest of international credibility. What is needed from national governments and regional bodies are firm proliferation policies for at least such data processing procedures, soft- and hardware which are explicitly to be used for screening, surveillance and discrimination. This is not the first time this point has been raised. After all, on a national basis governments have to ensure that data protection principles are being observed when government processing is outsourced. The proliferation of powerful dual-use technologies is subject to similar rules.

Such policies on proliferation would certainly help to raise the credibility of the universal principle of data protection particularly in such countries where citizens are faced with consequences of such soft- and hardware without the benefits yet of a data protection environment.

c) The reciprocal adjustment technique

While the previous suggestion referred to the export of data processing knowledge and technology to countries without or with insufficient data protection the reciprocal mechanism will continue to show their effects for countries which are recipients of personal information exports without having adequate protection in place. There is some hope that at least some of these countries will become weary of having to find solutions on a case-by-case basis.

But the focus of the debate is slowly shifting now. I have alluded to these changes before: In the past countries adopting data protection regulations may have done so - perhaps reluctantly in the beginning - so as not to be left out from the economic benefits of transborder data flows while still maintaining that perhaps culturally such rights were either not necessary or would remain a foreign element in their legal traditions. On the global level there is now - even more visibly than at the time of bi-polar tensions - a lingering question as to what extent global rights concepts conflict with local cultural values or special conditions and how such conflicts should be accommodated. This "local culture vs. universal rights" issue re-occurs in different contexts, be it freedom of opinion e.g., or women's rights, or the acceptability of the death penalty. And it does not spare data protection and privacy either.

Still - in my opinion - data protection will remain less affected by these controversies. From the experiences and the long tradition of regular conferences like these we experience that - despite different legal traditions and contexts which reflect different cultural values - a common core of values and practices has been emerging. One reason for this conformity in the face of the differences is - in my view - the similarity in

---

[16] See also: EPIC Statement of 17 June 2004 on the Cybercrime Convention at http://www.epic.org/privacy/intl/senateletter-061704.pdf.

essence of the challenges posed by information and communication technologies to societies all over the world.

Still, against the background of the value debate one has to remain cautious when the "cultural element" is being introduced. One has to learn to differentiate between cases where the cultural argument is misused for maintaining discriminatory practices, and cases of truly cultural concerns often stemming from the experience of a digital divide which makes it difficult to adequately meet the challenges of information technology. Bilateral and multilateral assistance practices have been in place and should further be extended to address the digital divide and the data protection divide simultanmeously.

d) Webs of communication

Visibility and transparency are essential factors of communication in national as well as in international environments and continue to be an essential element for a global data protection strategy. But visibility and transparency are not identical.

Visibility is necessary to provide orientation for national governments, international bodies, NGOs, companies and citizens. For enhancing visibility it becomes increasingly important - particularly for "temporary organizations" like this conference to present a clear and stable interface to the world which stays operational between conference dates and provides a highly visible direct access point , of course, on the net. On a regional level such concerns have already been realized and expressed in the strategy paper of the Art.29 Data Protection Working Party in September of last year.[17]

Transparency needs visibility to be functional, but it goes beyond that: Transparency is necessary for reaching and maintaining legitimacy .Any such one point information counter for global data protection cooperation of data protection agencies has there also to provide information at least on

- who is involved in providing such information,
- what internal procedures are implemented to ensure information quality,
- who are the sources of legal and expert advice, what is their competence, what are their interests.

2. Supplementary strategies

The development of data protection towards a global concept takes place in an environment of constant technological, economic and social change. These changes have their impact on any global strategies for data protection. They require constant training, attention to technological changes, and, perhaps a new alliance to make data protection better heard in the international arena.

---

[17] Article 29 Data Protection Working Party. Strategy Document adopted on 29 September 2004.11648/04/EN-WP 98, p.6.
http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2004/wp98_en.pdf

a) Looking for allies: a tripartite approach

International companies already have a global experience both with the handling of personal data as with interactions with various government authorities. Their experience has been used as soon as the reciprocal implications of data protection had become visible. Dialogue with large international companies had been important in developing e.g. the OECD Guidelines and accompanies the work of the Art.29 Group of the European Union. These co-operations were not free from diverging views as it is common in the area of business regulation. But in any case, these co-operations did not need any specific strategic efforts, at least not on behalf of data protection authorities.

Having mentioned the Art.29 Group leads to mentioning the current discussions on "Binding Corporate Rules", a discussion in which the Art. 29 Group just recently has emphasized its independence and "freedom of movement".[18]

This discussion has introduced a new quality of international co-operation which may have far reaching effects on the global career of data protection as a human right. This is neither the place nor is there the time to discuss in detail the relationship between international human rights and private sector operations, nor to go into more detail as to the various elements of the "Binding Corporate Rules"-approach. Also one could read this concept as modified re-run of the "contract clause"-approach, but I think we are faced here with a more far reaching change: While "Binding Corporate Rules" are still closely bound to legal requirements - and EEA data protection commissioners want to be assured of this - international corporations seem to be feeding now more expressly their normative condensate of global data protection into the process rather than starting from a particular national or regional concept.

Non-governmental organizations and citizen interest groups, from a different angle, have been using a similar approach, when regularly assessing the progress of data protection world wide, as e.g. in these renown annual reports by EPIC.[19] They, too, in their assessments do not start from a particular national or regional concept but apply what they see as an international standard of good privacy.

In the interest of the global debate on data protection it seems useful that data protection agencies - as assembled in this conference - provide a more explicit platform for a tripartite discussion among data protection agencies, NGOs and international companies on these global understandings of data protection to use their joint influence to move UN institutions towards a more binding and enforceable environment for data protection, may it be in the interest of human rights or also to create a more level playing field for adequately serving international customers and clients.

---

[18] See recently: Article 29 Data Protection Working Party. Working Document Establishing a Model Checklist Application for Approval of Binding Corporate Rules Adopted on April 14th, 2005. 05/EN-WP 108 - http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp108_en.pdf.

[19] Electronic Privacy Information Centre: http://www.epic.org.

b) Assessing the role of technology

Following developments in information and communication technologies is an ongoing task of national data protection agencies. Technology is of threefold importance: Technology - in its social context - poses the challenges that have to be answered by data protection policies; such answers can usually not be found directly in data protection laws, because these laws - increasingly so - attempt to remain technology neutral. At the same time information and communication technology can provide solutions which if embedded adequately into organizational and social practices can contribute to provide solutions for data protection concerns or at least can test the data protection commitment of those implementing such technologies. And finally information and communication technologies, in spite of their apparently open and inviting design have to constantly produce information on their operations to keep these operations functional; these processes create control information which in turn produces new challenges for data protection policies.

Furthermore, in the process of economic globalization and international co-operation between governments these technologies now are spreading with enormous speed around the globe. As the example of RFID has shown us there is no longer a proliferation cascade from the highest developed country to those still in the developing process. Such technologies are implemented simultaneously regardless of the stage of development, or at times even pre-tested in less developed countries before being globally implemented.

While in the past data protection authorities of the higher developed countries would assess the impact of these technologies and provide guidance, which within a suitable time would reach other countries to prepare them for coming challenges. this is now no longer adequate.

These developments require assessment capacity and capability which have to be pooled on a global level. Usually such shared advice was available through international conferences. Occasionally institutions like the European Commission or the OECD would provide venues and resources for such matters, as e.g. in the case of cryptology or privacy enhancing technologies.

I am afraid, this will no longer suffice to ensure the international viability of technology savvy data protection concepts; some institutionalized format for pooling available resources of data protection agencies on an international level will have to be found, perhaps by more systematically dipping into the resources of technology assessment institutions world wide, which are in the process of developing their own forms of international co-operation and observation.[20]

---

[20] See e.g. the function and role - in the European Union context - of the Institute of Prospective Technology Studies (IPTS), Sevilla - http://www.jrc.es/home/index.htm.

c) Enhancing international training

Both supplementary strategies discussed so far deal with expertise and experience. Expertise, experience and new knowledge are key factors for the successful operation and cooperation of data protection authorities on the national, regional and global level.

Not all of the data protection authorities have sufficient resources to provide for such comprehensive learning opportunities on a regular basis for their personnel. New data protection authorities need compact and readily available advice to bring them on the level of the state of the art. Such help has been provided. But this is not enough for the future. There should be mechanisms in place and already operating programs should be further be enhanced to provide resources as well as opportunities to improve the training of data protection officers. In this context it is also crucial - for the global reach of data protection - to further develop exchange of personnel between data protection authorities and doing so across cultural regions.

In my view such exchanges should, by the way, not be restricted to exchanges among data protection authorities. Nationally, regionally and on a global scale data protection authorities should be encouraged to exchange personnel with e.g. law enforcement authorities or e.g. private sector operators each within their organizational possibilities and practicalities. Such programs may perhaps pose logistic, if not legal problems, and certainly problems of organizational culture, but such envisaged problems should not discourage institutions to search for solutions.[21]

3. The core task: Strategies of substance

If - as I have suggested - we are at, indeed, a turning point, then all the traditional and even the supplementary strategy considerations have to be further supplemented by what I would call "strategies of substance".

Strategies of substance aim at reflection, discussion and promotion of the basic principles of data protection in a changing world. Two such strategies of substance will briefly be introduced to serve as examples and to invite further sugesstions:

- a strategy to supplement - on a global level - data protection with access to government information principles to answer the fundamental power shifts associated with information and communication technology more efficiently, nationally as well as internationally, and
- a strategy to revitalize - through re-reflection - data protection concepts on the basis of data protection practices.

---

[21] See also the suggestion of the Nigerian Cybercrime Working Group Co-ordinator at the ITU WSIS Thematic Meeting on Cybersecurity, Geneva, 28 June - 1 July 2005 at http://www.itu.int/osg/spu/cybersecurity/index.phtml.

a) A globally integrated concept for data protection and access

The global future of data protection is closely linked to an adequate approach to international information and communication systems handling personal data. It is the term "systems" which is essential here. On the national level data protection agencies have realized the importance of participating in the planning, design, implementation and operation of such systems. Influencing systems requires transparency. More and more countries have drawn consequences from the importance of government transparency for the awareness and understanding of such systems installed by governments and between governments .E-government concepts - also incorporating international exchanges - are being supplemented by e-democracy concepts ensuring transparency. Transparency laws - even older than data protection laws - have started long ago to extend around the globe. It is only until fairly recently, however, that the close connection between data protection and access to government information has received due attention. Several features of data protection laws contribute to transparency, and access to information laws contribute to data protection laws with their privacy conscious exemptions and the systemic transparency they seek to provide. And, indeed, in the context of national legislative changes, more and more agencies of data protection have also become responsible for overseeing transparency laws. Some countries and provinces in fact already operate on the basis of highly integrated access and data protection laws.

Access agencies cooperate internationally in a similar manner as data protection agencies.[22] For access laws, however, the international situation is still different. While the international human rights instruments which I have mentioned in the context of privacy and data protection do mostly acknowledge at least the right to seek and impart information, there is no generally acknowledged international right to access government information - with the exception, perhaps, of the Aarhus Convention, a UN instrument restricted, however, to access to environmental information.[23]

A joint effort - in a first step perhaps best expressed in a joint international conference of data protection *and* access to information agencies around the world on the need of a solid link between data protection and access rights - could give this issue further weight in the international human rights discussions. At the same time such a joint conference

---

[22] See the report on the Third International Conference of Information Commissioners in Cancun in February 2005 by Goldberg, David in Open Government. A Journal on Freedom of Information at http://www.opengovjournal.org/journals/journalindex.php?action=dumpfile&binarytable=Articlepdfs&article_id=512&file_id=66&journal_id=15&dumpfile=1&PHPSESSID=12e962b5a6ab6308e9eb1dcb4d8ac813.

The 4th Conference will be hosted in Manchester (UK).

[23] On this situation: Sutton, Graham: Freedom of information and data protection: reconciling conflicting objectives, in: Open Government. A Journal on Freedom of Information at http://www.opengovjournal.org/journals/journalindex.php?action=dumpfile&binarytable=Articlepdfs&article_id=510&file_id=64&journal_id=15&dumpfile=1&PHPSESSID=12e962b5a6ab6308e9eb1dcb4d8ac813

could help to reduce misconceptions and prejudices about the relation between these types of regulation which still exist in some countries.

b) Re-reflecting on Data Protection

To ensure the working of data protection principles in daily conflicts, to feed these principles into judicial procedures, to oversee their implementations by administrative oversight produces leads - over time - to a highly differentiated corpus of guidelines, regulations, general and special sector laws, court decisions and expert opinions which all make it more difficult to rediscover the underlying basic principles. These processes of bureaucratization - and I use this term here only descriptively, not pejoratively - are inevitable. Every handbook of organization management lists possible remedies to avoid such processes getting out of hand.. At the same time negative effects on the global understanding of data protection cannot be neglected. The history of human rights has shown that even human rights concepts need vision, and that such vision is essential for their global success.[24] And it is this vision which is at stake.

We have become slightly cynical with regard to visions. We have watched too many while they were being produced, and we have seen too many when they failed. And - it seems data protection has always relied a little bit more on dystopias than on utopias.

In this situation, I suggest. it would be helpful to set aside again some time and resources for a basic re-reflection on the substance of data protection. This suggestion is not aimed at yet another round of philosophical contemplation- even if this time more decidedly across cultural boundaries - on the universal value of privacy in the information age. Such activities have their use, they have accompanied the implementation of data protection and will continue to do so without the need of a special strategic intervention.

Rather, I would suggest a more careful attention to what data protection agencies know best, their daily practices. As in the early days of data protection when agencies and their procedures had to be designed and refined, the careful on the spot comparative analysis at those agencies already in operation had helped to develop more refined organizational models, and, even more so, had helped to shape a common professional ethos regardless of the national particularities these agencies had to observe.

It is time for another set of such exercises. Although it seems paradoxical to look more closely into details to meet the challenges of differentiation, a careful comparative look at these details might help to regain a better understanding of the underlying principles across cultural boundaries. It is easy to agree on principles, but there is the danger to loose them among the details. Now it seems time to look at the details to recover the principles again. While some of such work is already being carried out on a regional level, in the preparation of the Art.29 Group's issue papers e.g., and while some non-governmental organizations have contributed to this task from the outside, it seems

---

[24] On the importance of vision in the international human rights context: Lauren, Paul Gordon (2003). The evolution of International Human Rights. Visions Seen. 2nd edition. University of Pennsylvania Press: Philadelphia..

useful to undertake such comparative exercises more pointedly across regional boundaries and to combine these efforts with those efforts I had already mentioned in the context of training strategies.

The careful attention to detail and difference, in such exercises, I am convinced, will once again provide that fertile environment in which common concerns and experiences can revitalize shared visions.

It will also help - if undertaken broadly enough - to place culturally influenced viewpoints - like my own in this presentation - into the appropriate context.

V. Conclusion

All these reflections on strategies for a global acceptance of data protection are not without risk.

There is no guarantee e.g. that in spite of all current peer pressure and unity displayed at events like this different political developments in different countries and even within hitherto homogeneous regions will strain the solidarity among data protection commissioners in their strive for global principles. These strategies for global data protection and their very legitimacy will then be severely tested, and data protection agencies will have to answer to a global audience what importance they do assign to data protection principles, independence, transparency and solidarity.

In many places around this lake important decisions of global relevance have been made. Not all visions guiding such decisions have turned into reality. In many cases women and men had to reassemble again in these places to seek to mend what had become destroyed.

It is this spirit of persistency, this will to carry on with what has been seen as beneficial for the global society regardless of all set backs which - I believe - will be the most important element for the future global progress of the data protection idea, important beyond all strategies that we can devise.

Thank you very much./--

Note on the author:

Herbert Burkert is Professor for Public Law, Information and Communication Law and President of the Research Centre for Information Law at the University of St. Gallen, Switzerland. He is also Senior Researcher at the Fraunhofer Institute for Media Communication, St. Augustin, Germany (currently on leave of absence) and an International Fellow of the Yale Law School Information Society Project, New Haven, USA. - He can be reached at hb@herbert-burkert.net.