Notes on Contributors

Yaman Akdeniz is Founder and Director of Cyber-Rights & Cyber-Liberties (lawya@leeds.ac.uk) and Lecturer at the University of Leeds Faculty of Law, where he is a member of the Cyber-Law Research Unit. His publications include *Internet, Law, and Society* (coeditor, 2000).

Joe Bailey is Professor of Sociology at Kingston University. His publications include *Social Europe* (ed., 1998), *Pessimism* (1988), and "Some Meanings of 'The Private' in Sociological Thought" (*Sociology* 14:3, 2000).

Péter György is Professor of Aesthetics and a member of the ELTE Media Centre at Eötvös Loránd University.

András Kovács is Professor of Nationalism Studies and Jewish Studies at Central European University, and Professor of Sociology at Eötvös Loránd University. His publications in English include "Jews and Politics in Hungary" in *Values, Interests and Identity: Jews and Politics in the Changing World* (1995).

Lawrence Lessig is Professor of Law at Stanford Law School. His publications include *The Future of Ideas* (2001) and *Code And Other Laws of Cyberspace* (1999) as well as articles on cyberspace regulation.

László Majtényi is Parliamentary Commissioner on Data Protection and Freedom of Information in Hungary.

Dominique Memmi is Director of Research at the Centre National de la Recherche Scientifique (CNRS). Her book on contemporary law regarding decisions concerning life, death, and the body, *Dire, Faire Dire,* is forthcoming in 2003.

Nils Muiznieks is Director of the Latvian Center for Human Rights and Ethnic Studies. He is the author of numerous publications and also a regular contributor to the annual UNDP publication "Latvia. Human Development Report."

Mark Neocleous is Lecturer in Politics at Brunel University and coeditor of *Radical Philosophy.* His publications include *The Fabrication of Social Order: A Critical Theory of Police Power* (2000) and *Imagining the State* (forthcoming 2002).

Renata Salecl is Senior Researcher at the Institute of Criminology of the Faculty of Law at the University of Ljubljana. She is the author of *(Per)Versions of Love and Hate* (2000) and *The Spoils of Freedom: Psychoanalysis and Feminism after the Fall of Socialism* (1994).

András Sajó is Professor of Legal Studies at Central European University. His publications include *Limiting Government: An Introduction to Constitutionalism* (1999) and *Political Corruption in Transition: A Sceptic's Handbook* (coeditor, 2002).

Ensuring Data Protection in East-Central Europe

BY LÁSZLÓ MAJTÉNYI

For a constitutional lawyer who lives in Western Europe or across the Atlantic, it may be surprising that while data protection is rarely mentioned explicitly in Western constitutions, the right to the protection of one's personal data is guaranteed almost without exception by the constitutions of postcommunist countries as both a citizen's right and a human right.[1] It is true, however, that the constitutional insertion of such stipulations often is no more than a symbolic gesture reinforcing the break with communism—that what these provisions circumscribe is often not so much a right that can be properly enforced but are instead a singular expression of the goodwill and remorse of the state, both of which may well sink into obscurity over time. The postcommunist nations must also learn, or rather relearn, that the law is not primarily the encryption of the demands the state may put on its citizens, but rather the citizens' guarantee for protection from the powers of the government and private enterprise in what we might call a face-off between Big Brother and Little Brothers.

It is also a surprise that, in the process of overhauling their political systems, a few Eastern European countries have enacted information legislation years before parts of Southern Europe.[2] Yet in some of these countries the progress of the law stopped in its tracks, and a genuine culture of data protection has not evolved. In these countries, the further development of

data protection may receive fresh impetus from their impending accession to the European Union. But these hopes entail difficulties on their own. National legal systems often take shape in response to external influences, but these influences are most beneficial only when they are coupled with interiorized values.

In this respect, the legal history of East-Central Europe justifies great expectations. Hungary is in an especially advantageous position. While the protection of personal data and the institutions of freedom of information remain under attack, the country had mounted, even before the fall of the old regime, major intellectual efforts to foster a culture of data protection. These efforts went beyond publishing studies and translating literature to informing and moulding public opinion.[3] They conveyed the barely concealed political message that it was possible, indeed necessary, for the individual to counter the omnipotent state. In Hungary, society has been uncommonly receptive to the idea of data protection because the creation of legal institutions went hand in hand with the ethos of undermining the political system, and also tied in with a century-old tradition of citizen's rights and individual protection that was still very much alive in the minds of people. Surveys have shown that, in more than one East European country, the cause of data protection enjoys the massive support of the public.[4]

In what follows I propose to review solutions advanced by four countries in the region that have made considerable efforts recently, in harmony with European legal progress, to develop their own data protection laws. Some of these countries embarked on a slower-paced but organic path of development, while others have seen very abrupt changes. Yet all share in the effort to narrow the gap between their laws (including their legal practices) and the principles of the European Union directive.

The Czech Republic

New Czech legislation was passed just before this manuscript was completed. It is therefore worthwhile to review the provisions of the local data protection regulations effective before this new enactment, not least because this law was retained in the Slovakian legal corpus after the separation of Czechoslovakia into the Czech Republic and Slovakia in 1993. Slovakia has since enacted new legislation as an independent nation (which will be discussed later). The Czechoslovakian law preceding these separate developments is thus deserving of a look if we are to follow up on legal developments in the area.

The Czech (originally Czechoslovakian) data protection law was adopted in 1992.[5] The right to have one's personal data protected is also guaranteed by the constitution. Under the human rights charter of the Czech constitution, every person is entitled to protection against the unlawful collection, disclosure, or other misuse of personal data (Czech Constitution, Art. 10(3)).

The Czech law was binding for records both automated and manual, including those maintained by the entire public sector. The law expressly provided for its application to other records regulated by law, such as information processed by the secret services, and private databases. Interestingly, the country's penal code makes a distinction between crimes against the protection of data (Section 178) and the use of information for business purposes when the information does not qualify as a business secret (Section 128).

As defined by the law, data subjects are individuals but not legal entities. In essence, the law must be applied to sensitive data only. This category of data, however, is somewhat broader in its scope than either in Convention 108 of the Council of Europe or the EU directive, since it implies that it covers information pertaining to racial origin, nationality, political views, membership in political parties and movements, religious views, criminal records, health, sexual life, financial situation. Although the law does not

explicitly mention membership in trade unions, the trade union structure of former communist countries would lead us to argue that such membership should be included in the category of political affiliation. By contrast, I believe it is a fundamental error to make property issues part of what constitutes sensitive data. At any rate, the only so-called information systems that had to be registered under this law were those that contained a record of sensitive data.

As another rule, in the Czech Republic no record of sensitive data could legally be kept unless as expressly allowed by law or as consented by the subject concerned. This implied, however, that subjects were not entitled to their right to informational self-determination with respect to all their personal data. In what we might term a case of grave negligence, the law appears to have protected sensitive data only. The act further stipulated, short of consent obtained, that the record had to offer guarantees of dignity, personal honor, and good reputation. This meant that it was possible to keep files on a wide range of sensitive data even without the consent of the subject, citing the unavailability of such consent.

The regulation of sectoral data protection is not well advanced. In the banking sphere, legal stipulations cover the transfer of personal data, including civil and criminal proceedings and procedures brought by the tax authority (Act No. 21/1992 on banks). In contrast, credit data appear to be unprotected by the laws. The tax law does provide for the transfer of personal data (Act No. 337/1992), while the handling of health information is only governed by an order of the competent minister (Methodical Instructions on Data Protection in the Medical Information System, 1994). The protection of personal data used for statistical purposes is governed solely by the guidelines issued by the head of the Statistical Bureau (No. STO 8/1996). These shortcomings fly in the face of the general requirement that sectoral data protection, especially when certain rights are restricted, must be provided for in legislation adopted by parliament.

In evaluating the former status of data protection in the Czech Republic, I believe that the lack of an independent monitoring body was far more objectionable than the fact that the regulations did not tally with the substance of the EU directive. As late as 1996, the government threw out a proposal in which the Ministry of the Economy sought to establish such an independent body, which would have reported to the cabinet. The breakthrough came in January 1999, when the Czech government moved to harmonize the country's data protection law with the EU directive and, as part of that effort, to set up an independent organization (Czech Republic Government Resolution No. 70 of 27 January 1999). In April 1999, the European Parliament issued a resolution urging the Czech Republic to adopt a new data protection law (Privacy and Human Rights, 1999: 63).

A law passed in 1996 empowers Czech citizens to access secret service files collected on them by the national security agency run by the former communist regime. Foreigners, however, are not entitled to these data, even if they had been the targets of such surveillance at one time.

Yet on the whole Czech society seems to be sensitive in its responses to the abuse of personal information. A case in point was the nationwide scandal that broke out in 1992 when it was revealed that the Interior Ministry had sold to Procter and Gamble the personal data of every infant under two years of age and every woman aged 15 to 35—a total of 2 million Czech citizens (the information was used in a direct marketing scheme). In 1996, CD-ROMs surfaced on the black market that contained the unlisted phone numbers of several persons, including Czech President Vaclav Havel. (Similar abuses were committed in Hungary; in Poland, phone numbers were used by national security.) Society's demands are illustrated by a 1997 poll in which 79 percent of the respondents considered privacy a fundamental value. In 1998, 75 percent believed that their personal data were being abused, and two out of every three persons identified data protection a major issue.[6]

The New Law

As the latest and very welcome development in the Czech Republic, on April 4, 2000, the Czech parliament enacted the country's new data protection law (Act No. 101 of 4 April 2000 on the protection of personal data and on changes to several laws). Since the act only became effective on June 1, not enough time has passed for a body of legal actions taken under its auspices to accumulate that we might discuss. The law applies to all automated and manual records kept by the national government, local governments, individuals, and legal entities, unless provided otherwise by the law itself. Such exemption from the force of the law is granted fully to statistical and archival records, and partly to the secret services, the police, the national Interpol center, the Ministry of Finance, and the Ministry of the Interior. From my perspective, the law is extremely lenient when it comes to law enforcement agencies, exempting them from the rule of purposefulness in processing information and the heightened protection of sensitive data.

The law establishes nonpecuniary liability for damages to the subject's dignity, honor, and good reputation. Whenever such damage arises in connection with employment, it will be governed by the labor code, while compensation is subject to the civil code and the commercial code (Act No. 40/1964 Coll., on civil code; Act No. 513/1991 Coll., on commercial code). In this respect, the Hungarian law is more stringent insofar as it establishes objective liability for data controllers misusing information. (This stringency is informed by the Hungarian legislators' assumption that the data controller is invariably in a more powerful position than the wronged subject.)

The act finally created the Office of Data Protection (Chapter IV, "On the Position and Competence of the Office"), an independent authority subject only to the country's laws and other legal instruments (unlike its Hungarian counterpart, which is only answerable to laws passed by parliament). As an important

guarantee of the office's independence, a separate chapter in the state budget is devoted to its business management. (Similar to Hungarian law, where the three ombudsmen are discussed under the same chapter of the budget. Incidentally, in the future the budget allocation proposal should be submitted to parliament not by the minister of finance—who has come under repeated criticism by the data protection commissioner, among others—but by the Human Rights Committee, based on the proposal of the ombudsmen.) The office monitors enforcement of the law and runs the data protection register, which everyone is free to inspect. It also prepares an annual report that it sends to the House of Representatives, the Senate, the cabinet, and also to the office bulletin for publication. Regrettably, the Czech parliament—unlike the Hungarian body—does not discuss the report in a plenary session or adopt it by vote annually.

The office is headed by a chairman, who is appointed by the president of the republic on the recommendation of the Senate for a term of five years. The appointment is renewable for one more term only. The creation of the office significantly increases the chances of effective data protection.

Slovakia

Slovakia's 1998 data protection law is the result of several years' work.[7] Legislators who drafted the bill studied a number of foreign models, including the experiences of the Hungarian Bureau of the Data Protection commissioner and our legal solutions. This act clearly bears the stamp of the EU directive. Remarkably, the consent of the data subject is given more detailed treatment than by the Hungarian law, which merely prescribes such consent. The Slovakian version follows the EU directive more closely by defining consent as "the freely and unambiguously expressed will of the subject consenting to having his or her data processed" (Art. 3 f). Also in tune with the directive, the act declares trade union

membership to be sensitive information (Art. 8). Furthermore, it makes the transfer of data abroad subject to adequate protection (Art. 18), and it differentiates between data controllers and data processors.[8]

The law does not simply place the function of the data protection commissioner in the hands of the government—which is somewhat of a risky move in East-Central Europe—but it seems to go beyond this Western model in its drive to deeply embed the commissioner in executive power. The commissioner is appointed and relieved of his post by the government, on the recommendation of none other than the chairman of the Slovak Statistical Bureau (Art. 26 (1)). However, the commissioner, once appointed, cannot be removed from office unless there is a proven conflict of interest, or he or she fails to perform his or her duties for more than a year, or if he or she is found guilty of an intentional felony. The commissioner acting in office is answerable only to the law.

The commissioner submits his annual report to both the government and the parliament, but the latter does not discuss that report. The commissioner's bureau forms an independent unit within the Government Office (Art. 27). Its officials are bound to the Government Office in a legal relation, which means that they are not appointed and employed by the commissioner, or if they are, the commissioner merely practices that function as delegated to him by the Government Office.

Surprisingly, under the Slovakian law, the data protection register is not run by the commissioner but by the Statistical Bureau of the Republic of Slovakia, and not even by the chairman at that (Art. 19 (1)). Similar to international norms and the Hungarian solution, mandatory reporting to the register applies to the public and the private sector.

The Statistical Bureau can extend help free of charge to the supervisory authority, which is the data protection commissioner in his work. The data in the register are public. Some countries, such as Great Britain, outsource the maintenance of the register,

but even in these cases the commissioner remains in charge of the register, while those actually running it are merely considered data processors. Experiences in Hungary indicate that the Statistical Bureau, as one of the organizations acquiring the largest quantity of personal data, is prone to violate the constitutional protection of privacy by virtue of its rational interior processes. In the Slovakian model, the commissioner should expect to face an especially difficult situation whenever he is called on to confront one of the largest data controllers, the Statistical Bureau. Presumably, this contradictory setup stems from the initial idea in Slovakia to integrate the tasks of data protection within the organization of the Statistical Bureau. Although at a later stage, perhaps in an effort to follow the guidelines of the Council of Europe and the EU, an independent government authority came to be created, the initial concept was never fully abandoned.

The Polish Solution

Poland's new constitution became effective on October 16, 1997. The structure of basic informational rights in Poland has begun to look like it is moving in the direction followed by Hungary, and protection of these rights has been articulated at the constitutional level. (During my visit to Poland in 1995, I found that data protection at the time was not the focus of professional interest and debate, as it was in Hungary. Invested with a rather broad and general competence, the ombudsman did not deal with too many cases involving data protection. In one of the cases he did deal with, he investigated whether it was legal to require mandatory registration of bicycles using the personal ID number.) The protection of data is provided for in §47 of the new constitution, which declares that "everyone is entitled to legal protection of his own and his family's privacy." It follows from the diverging philosophies informing Poland's and Hungary's respective basic regulations of this field that the Polish constitution

includes specific details on providing for the protection of privacy. In fact, the Polish constitution may well be the most meticulous in the world when it comes to rules of data protection. Beyond guaranteeing protected communications by upholding correspondence and telecommunication secrets (§47), the constitution affirms that citizens may not be forced to supply data about themselves except as allowed by law. By the same token, administrative bodies may not collect, store, or disclose data about citizens, except when doing so passes the "necessity test" of democratic government (§47 (2)). Everyone is entitled to access and to inspect official documents and files kept on him or her. Another right guaranteed by the constitution is the right to correct or delete data in official files that are inaccurate or were collected illegally. Beyond the practical significance of legal protection, Polish legislators undoubtedly invest a symbolic importance to this law as a depository of fundamental rights—something that happened under very similar circumstances in Hungary a few years ago (Platten, 1998).

The Polish law applies equally to information processed manually.[9] While its effect extends to the public and the private sector, it does not apply to data processed by individuals for personal purposes.

In defining sensitive data, the act goes beyond the usual standards and makes specific mention of the genetic code as well as alcohol and drug addiction. Data subjects are entitled to know the source and nature of their information data controllers keep on file or transfer, and they have the right to request copies of the record.

The Polish Inspector General of Data Protection (Generalny Inspektor Ochrony Danych Osobowych) oversees a bureau whose independence is more overt, making it unlike the Slovak solution but quite similar to the Hungarian model. The Polish inspector is appointed for a term of four years, which can be renewed once. He enjoys immunity from government interference, and cannot be replaced or removed from office except in special cases (with

the approval of both houses of parliament). His sphere of competence follows international norms, and is akin to that of his Hungarian colleague inasmuch as it enables him to evaluate draft legislation and statutory instruments pertaining to data protection. He prepares an annual report to be filed with the Sejm, the Polish parliament. The inspector is also in charge of running the data protection register, and may launch inquests ex officio or upon receiving complaints. An unusual caveat, as pointed out by Nick Platten, may interfere with the efficacy of the protection available from this institution: the inspector does not have the right to investigate complaints objecting to the use of data that do not have to be reported to the register (Platten, 1998: 6).

The constitutional standing and legitimization of the inspector general indicate a specialized parliamentary ombudsman akin to its Hungarian counterpart. At the same time, while the inspector's powers of investigation are much narrower, his or her competence is much broader than either that of the Hungarian commissioner or that typically assigned to ombudsmen: it is more like the competence of a public administrative body. The rules applicable to procedures conducted by the inspector are those of the administrative procedure code. He may issue an administrative decision that is binding for the data processor in violation of the code, and even levy a fine for misdemeanors (Millard and Ford, n.d.). Consequently, the opportunities for legal redress are also rather peculiar. If the data processor found guilty is not happy with the inspector's decision, he may petition the inspector himself for a review. Appeals of the decision are heard by the Supreme Administrative Court. In short, we may describe the body created in Poland as that of an ombudsman in terms of its separation and independence, but in other respects as more like an administrative organization.

Liability for damages is spelled out in the civil code. Data processing is regulated by a number of sectoral laws, albeit these are not sectoral data protection laws themselves.[10]

The act regarding Files Kept by Communist Secret Police provides for the creation of a National Remembrance Institute destined to uphold the victims' right to informational self-determination. The bill was first vetoed, but then ultimately signed by President Aleksander Kwasniewski. The institute was finally set up in the summer of 2000, but its newly elected president, Leon Kieres, claims it will take months before actual operation begins.[11] Under another act, Poland is looking into the career of current government officials as former agents. By 1999, more than 2,300 such investigations had been completed (Privacy and Human Rights 1999: 129).

Hungary

The most conspicuous feature of the Hungarian act [12] is that it stands as the first informational rights law in Europe, insofar as it regulates data protection along with freedom of information, treating the two rights in a reciprocal interpretation and assigning them to the protectorate of one specialized parliamentary ombudsman.[13] The constitutional revolution in Hungary created the right climate for this solution, one that had been proposed for some time by international scholars. The act is also an expression of the legal philosophy behind Hungary's shift for democracy in that it breaks with the "tradition" that had long defined relations in Hungary between the state and its citizens. Under single-party rule, the state lacked transparency even as its citizens remained penetrable to the eye of power. The avowed mission of the act was to reverse this order of things by rendering the state transparent to the public and the citizens aloof to scrutiny.

Discussed here only in its data protection provisions, the act employs a number of technical solutions that reflect how far European data protection culture had evolved by 1992, the year in which the act was created. Its legal solutions are however more advanced than those involved in the 1981 Data Protection Con-

vention of the Council of Europe. The law was drafted without knowledge at the time of the language of the data protection directive issued by the European Union, which therefore could not have had a direct impact on the substance of the act. Nevertheless, it reflects an approach that is in kindred spirit to the directive's guiding principles. With most of what technical shortcomings it may have had now corrected through amendments, the Hungarian act has been inching closer to the directive. (To stress the importance of organic development, Hungarians prefer amendments and a series of sectoral laws to new legislation as a way of forging absolute harmony.)

The act includes the following:

- It is forbidden to use the all-purpose personal identification number (PIN) without restrictions.[14]
- Under the act, citizens are entitled to the same protection whether they face private or public data controllers. By the same token, the commissioner's powers of investigation are extended without restriction to data processed by the state, local governments, private business, and even individuals.[15]
- The act must be applied to automated and manually controlled records alike. When it comes to the unauthorized handling of data, even the media is not privileged, except for the single exemption of the press from the obligation to file with the Data Protection Register.
- The terms of modifying the DP-FOIA are unlike those of other acts, and are akin to the rules of amending the constitution itself in that they stipulate a two-thirds majority to approve any change. The act regulates the field with a focus on informational self-determination rather than on a protective right extended by the state. Typically, the legality of handling data rests on the voluntary consent of the data subject; without that consent, personal data can only be handled as allowed by the act or other legislation (namely by a statutory instrument of at least the rank of an act in the legal hierarchy of measures), or else in a very limited sphere, including,

for instance, by decree of local government on local community taxes. The handling of sensitive data is subject to even more stringent rules.

- The act applies equally to all forms of handling personal data. In view of the way in which the notion is construed, "data handling" means any form of manipulating and storing personal data by anyone or any entity (DP-FOI Act §2 (4)). The right to have one's data protected is granted to every individual, irrespective of citizenship status. At the same time, Hungarian law does not recognize the right of legal entities to this protection, which constitutes the single most important limitation of this personal right. Furthermore, the law offers no such protection for the rights of the deceased. The memory of the dead is protected under the civil code by what is known as the right to reverence, but the DP-FOIA does not in itself safeguard their personal data. There have been a few cases that called for intervention by the data protection commissioner to terminate a violation of this right, but these invariably involved living relatives implicated in the information at hand, who were thus the proper beneficiaries of the protection.

Those handling data in Hungary are mandated by law to have themselves listed in the data protection register. Personal data collected for the purposes of scientific or scholarly research cannot be used for any other purpose, and must be rendered anonymous to the extent allowed by the research objective at hand. If the consent of the subject is not given, researchers may only publish personal data if doing so is essential in displaying the results of a historical study or investigation.

The informational rights of the victims of secret services under the single-party state and the screening of government members are provided for in Act No. 22 of 1994 (On Screening Certain Prominent Officials and on the Institute for History). Under the act, such victims may access their files in specialized archives created for this purpose, such as the Institute for History, but the

data of other persons are deleted for the duration of the inspection. As a commissioner, I have repeatedly criticized this piece of legislation. I have, for example, objected to the freedom of the secret services' successors to decide at their own discretion, without external control, which of their predecessors' files they are willing to turn over to the Institute for History.[16]

I have also taken issue with the act for lumping together and treating as equals former victims and informants. More than for moral reasons, this move is problematic because of its distribution of informational rights, since traitors are always aware of their deeds—unlike their victims, from whom those deeds have remained hidden.[17] The range of government officials to be screened was at first given a narrow definition by the act; it was practically limited to checking for the secret service ties of those who must by law take the oath before the National Assembly or the president of the republic. An amendment to the act, passed in 2000, effects a major extension of that circle to include the entire staff of judges and prosecutors, as well as senior media leaders. In addition, certain professionals, such as attorneys, notaries, and clergymen, may request to be screened on their own.

Since the general DP-FOIA took effect, parliament has passed and modified a number of bills specific to sectors.[18] For example, the act does not distinguish between the concepts of data and information. The act also specifies two groups of sensitive data. The first cluster includes information pertaining to racial origin, nationality, national or ethnic origin, political opinion, and religious or other belief. (As potentially implying political conviction, trade union membership is also tacitly understood to be in this category, if not explicitly specified as such by law.) This information can be handled only with the written consent of the subject, or when doing so is mandated by law in the interest of enforcing a basic constitutional right, or in the interest of national security, criminal prosecution, or the prevention of crimes.

The second group of sensitive data consists of information pertaining to health, pathological addiction, sexual life, and criminal

conviction. The handling of such information is illegal unless based on the written consent of the subject or ordered by provision of law.

A 1999 amendment to the act added the concept of data processor (Act No. LXXII of 1999 on Modifying the DP-FOI Act), edging the law closer to the expectations of the EU directive. Data processor means any natural or legal person, as well as any organization without legal personality, that may engage in processing data on assignment from the data controller (data processing refers to the technical execution of data processing tasks under the supervision of the data controller).

Personal data may not be handled for any purpose other than as allowed by law, as a way of exercising a right, or to fulfil a legal obligation. The handling of data is not legal beyond the accomplishment of such purpose. The mandatory supply of data may be ordered by law if that serves a public interest. The data subject must be informed of the purpose of the processing, of the entity to be in charge of or processing his or her data, as well as whether the supply of the information sought is voluntary or compulsory. In official proceedings brought by the subject, the circumstances under which he or she gave consent to having the information processed must be reviewed and given due deliberation.

The requirement of data quality presupposes lawful and fair collection and processing of data that are accurate, complete, and current, as well as a method of storage and retrieval that is suitable to prevent identification of the subject beyond the necessary period of time.

The transfer or compilation of data is subject to consent or authorization by law. Not only may the public administration not be regarded as a seamlessly uniform data controller, but the lawfulness of linking databases must be submitted separately to the scrutiny of each administrative body. Data controllers are to take every technical and organizational precaution possible to ensure the security of information, and to protect the files from all forms of unauthorized access.

Data controllers are obliged to list their activities with the data protection register maintained by the data protection commissioner. The affidavit must state the purpose of the data processing, the range of subjects, the type and source of the information involved, the legal grounds for its control, as well as the deadline for deleting the data from the records. The register itself contains no personal data, since it works as the record of records (or a kind of metarecord), in full view of the public eye. Its function is to enable anyone to ascertain what records are kept by whom of their personal data. Although it is also instrumental for the data protection commissioner in his supervisory mission, in Hungarian law the register fulfills a role of registration rather than one of entitlement. There are types of controlling data exempted from the listing obligation, including employment or student status and relations, business-to-business relations, the sovereign data controlled by churches, health services, social security, welfare programs, proceedings at court or the prosecutor's office, statistical surveys (provided that the data are rendered anonymous), the press and the media, scientific research and archives, and data control by natural persons for their own personal purposes.

The right to informational self-determination is a privilege guaranteed by the Hungarian constitution, which means that individuals are free to decide whether or not to supply their personal data—unless their right to do so is limited or suspended by a provision of law. In addition, they are entitled to information on the fate of whatever information they have relinquished. Data controllers must clearly and intelligibly inform the subjects of their data under control or processing, the purpose, grounds, and duration of the data control, the address of the processor, and the nature of the processing or transfer. All this may be required by law, but at least for five years retroactively (and for twenty years for sensitive data). Requests by the subjects must be answered within 30 days free of charge, although a fee may be charged for those applying for information in the same field more than once in the course of the same year. Such information

may not be withheld unless doing so serves the interest of the state, including national security, the persecution or prevention of crimes, the financial interests of a municipality, or the dictates of protecting the rights of the subject or other persons. Should the information be denied, the reason for doing so must be communicated to the subject, and the data protection commissioner notified of all denied requests on an annual basis. Data controllers are required to update any inaccurate information they may have in their files.

Personal data must be deleted if their handling is unlawful, if the subject so requests as allowed by law, and whenever the purpose of the control no longer obtains.

In 1999, the Hungarian parliament publicized the Council of Europe's Data Protection Convention (No. 108), under the terms of which data transfer is to be considered lawful among the member states that have ratified the convention. Pursuant to Hungary's Archives Act, research of archival material before the expiration of limitations is permitted for researchers from countries guaranteeing the same level of data protection as Hungary, and whose justice ministers have made a statement to that effect that concurs with the data protection commissioner.

The commissioner for DP-FOI is elected as a specialized ombudsman by a two-third-majority vote of parliament, with a mandate renewable once. The commissioner observes the implementation of the DP-FOIA and other statutory instruments on data control, examines the complaints lodged with him, and maintains the data protection register. He monitors conditions to determine that the protection of personal data is upheld, together with the publicity of data of public interest. He presents proposals for the adoption or modification of legislation concerning such data and their handling (DP-FOIA §25).

An important duty of the commissioner is to evaluate draft legislation involving issues of data protection and freedom of information. In discharging his functions, the commissioner may request the data controller to furnish information on any matter,

and may inspect any document or records likely to bear on personal data or data of public interest. If he or she identifies a data handling practice as unlawful, he or she may instruct the controller to cease the activity in question. Should the data controller fail to comply, the commissioner may inform the general public of the illegal control of data, the identity of the data controller, and the categories of data involved.

The commissioner can also propose to narrow or broaden the range of data to be considered state secrets or official secrets. Any organization that believes its data categories qualify for official secrecy must seek the opinion of the commissioner. State secrets and official secrets cannot hinder the commissioner from exercising his rights, but the secrecy provisions are binding upon him as well. The commissioner shall exercise his rights in person in cases when the data qualifying as state or official secrets are controlled by the armed forces, the police, or the national security agencies (DP-FOIA §26).

Anyone may appeal to the commissioner to act on a supposed violation of his or her rights, or on an impending danger thereof, in the processing of his or her personal data or his or her access to data of public interest, except in cases in which the information is being handled in a judicial procedure or proceedings at court. Such applicants enjoy the same protection as those communicating matters of public interest.

Besides the DP-FOIA, there are other statutory instruments that regulate the duties of the commissioner.

Article 4 (4) of the 1995 Act LXV on State and Official Secrets provides that the opinion of the commissioner shall be heard in classifying data as official secrets (a stipulation also contained in the DP-FOIA). The list of data subject to official secrecy shall be published in the *Hungarian Gazette* (Magyar Közlöny). The draft of this list is referred to the commissioner, whose opinion must be accommodated in the final version.

Article 7 (3) of Act XLVI of 1993 on Statistics provides that the commissioner shall participate in the sessions of the Hungarian

Statistics Council as a permanent guest. The act also stipulates that, among other information, personal identification data may be connected with the database temporarily (namely when new information is linked), but the specific rules of such interconnection shall be determined in respect of the commissioner's opinion.

According to Article 6 (3) of Act No. CXIX of 1995 on Direct Marketing, the data controller is required to report to the commissioner, before embarking on the activity under Art. 28 (1) of the DP-FOIA, such data processing intent as may fall within the scope of this Act—except when it serves the purpose of scientific research and is not publicly disclosed (Art. 30. h of the DP-FOIA).

Act No. CXIX of 1995 also makes researchers, public opinion polls, market research, and direct marketing organizations liable for implementing the technical and organizational measures that may be necessary to ensure the maximum security of data processed by them. Those engaged in such an activity—except for scientific researchers—shall draft their own internal regulations of data protection and data security in a form that is approved by their professional representative organizations and by the commissioner, who gives an opinion on the legality of the data processing involved.

Data transfer abroad is to be reported to the commissioner before it takes place. The commissioner examines whether the conditions of processing the data abroad are adequate.

Besides the duties spelled out in statutory instruments, the commissioner has one further area of responsibility. This is to inform society about the concept of data protection, its value for individual citizens, and about their right to freedom of information. This implies working with local and national media, publicizing legislation, advertising the services offered by the commissioner and his or her bureau, and promoting teaching and research in the professional field.

In cases of supposed violation, the subject has the option to seek remedy from the commissioner or to go to court. Although the commissioner's procedure is free of charge and comparatively

speedier, it cannot conclude in a legally binding resolution, whereas a court verdict will be clearly enforceable. Those who claim to have suffered a violation of their rights are given the benefit of doubt in litigation.

In the first instance, it is up to the data controller to prove that the data have been controlled legally. When in doubt, it is presumed that the subject did not consent to having his or her personal information processed. If this is the case, objective responsibility accrues to the controller, who will be found liable for damages even if the wrong was not caused wilfully. This liability can only be preempted by an act of God, or by intentional vexation or grave carelessness on the part of the subject. The data controller is also held liable for damages caused by the data processor in its employ.

The penal code separately and expressly defines the violation of privacy, unlawful data control, the abuse of sensitive data, the violation of secrecy in correspondence, and computer fraud as felonies potentially carrying imprisonment.

As a major gesture of acknowledging Hungary's data protection law and its practical application, on September 7, 1999, the Working Party on the Protection of Individuals with Regard to the Processing of Personal Data recommended the commission to qualify Hungary as a country extending adequate protection.[19]

On July 27, 2000, the European Commission passed decisions accepting the United States as a "safe harbor,"[20] as well as recognizing the adequate level of protection in Switzerland and Hungary, thus freeing the flow of personal data from the EU to these latter two countries ("Data Protection," 2000).

Conclusions

The dilemma of the letter of the law versus effective data protection practice raises demands in postcommunist countries that appear quite specific. This specificity is only apparent, however,

because the same quandaries can be traced just as visibly in the history of Western and New World legal institutions with respect to the enforcement of fundamental constitutional rights. In my opinion, the only difference is that the conflict manifests itself on a more escalated level in the legal culture of the former Eastern bloc. The winner of the elections who hinders the vindication of informational rights in possession of his democratic legitimization and in the political interests of the day (of law enforcement, taxation, or of mere elbowing for position and power)—such an election is the exception in the West, but more like the rule in Eastern Europe. Here we must bring a serious skepticism to appreciate the existence of "independent" institutions reporting to the government, even as we must admit that the "old" democracies themselves would do better to divorce the task of data protection from administrative power. In the East, the official urging his government to abide by the law and the constitution may easily find himself out of a job. The political forces tend to regard the entirety of the administration as their sole possession, and senior officials are often more committed to the cabinet than to the law and constitution that put it into power. This makes it difficult to keep in mind that the rule of law is destined to assign strict limits to the maneuvering space of governments.

In closing, I would like to make five comments. The first concerns the creation of a system of data protection along the lines of the ombudsman, operating under, but not controllable by, the parliament, as the best chance for the enforcement of informational freedoms. Such an organization may be headed by a high-ranking specialized ombudsman whose mandate should be ideally longer than a parliamentary cycle as a means to ensure distance and separation from politics. His independence from politics could be emphasized by a rule for which I am aware of no examples. My idea is that the law could prohibit the reelection of a commissioner for the second term. As a downside, such a stipulation would dispense with a commissioner at the end of his tenure even if he has proved his excellence in office. On the

other hand, it would offer the advantage of preventing the commissioner toward the end of his term from yielding to the temptation to court the favor of executive and legislative power.

My second observation is about the need for an accumulated corpus of case law to supplement EU-conforming laws as a condition for truly efficient data protection. Such a corpus would demonstrate the possibility and power of enforcing privacy rights. Judicial practice must be coupled with the legal practice of the data protection commissioners, which is the best tool with which to shape public opinion and the attitude of data controllers.[22]

My third comment is simply that the number and rigor of sectoral data protection laws are very reliable indicators of a country's state of progress in the area of data protection.

Fourth, I think it amounts to unreasonable faintness of heart to be afraid of data protection scandals, citing a favorite East European misconception that by openly talking about violations we will damage the reputation of our country. Scandal and heated debate are normally followed by a process of purification, and their very public disclosure is proof not only of the existence but the proper operation of independent institutions. Countries with highly evolved data protection systems, like Iceland, Canada, and Great Britain, reverberate with the din from the government's and the market's violations of data protection principles. As the data protection commissioner of Hungary, every year I find myself in fierce dispute with the minister of finance over legislation granting excessive powers to the tax authority over citizens; with the minister of the interior over closed-loop camera systems installed in public areas and the extent of personal information requested upon crossing our borders; with the minister for secret services over illegal surveillance of citizens and inadmissible classifying practices; with the president of the Statistical Bureau over linking large state-controlled databases and the use of sensitive data in nationwide census. My bureau has been in constant conflict, in the full view of the public eye, with the major banks and insurance companies, telecommunications and mail order firms.

It was with this openness in mind that the decision-makers of the EU determined that Hungary indeed possessed adequate guarantees of data protection. Not only did these open debates delay that acknowledgement, but presumably they hastened that honor.

My fifth and final thought on Eastern Europe focuses on Hungary. I think that linking the cause of data protection with that of freedom of information is a good idea that has worked, both in terms of the law and on the organizational level. Beyond its benefits, which we have seen in Canada and, more recently, closer to home, this model may prove instrumental in solving the set of data protection problems that are particular to Eastern Europe as it leaves behind the great change of the region's political system.

Notes

[1]Czech Republic: Art. 10 (3); Estonia: Articles 42, 43, 44; Hungary: Art. 59; Lithuania: Art. 22; Poland: Articles 47, 51; Russia: Art. 23; Slovakia: Art. 16; Slovenia: Art. 35

[2] In 1992, a handful of East European countries adopted data protection laws (among them Hungary's DP-FOI legislation), some of which surpassed Western legal standards at the time in terms of their rigor and philosophy of regulation. A few years later, similar statutes were established in Italy (on December 31, 1996, No. 675, on The Protection of Persons and Other Entities in Relation to the Processing of Personal Data) and Greece (on April 10, 1997, Act 2472 of Greece on The Protection of the Individual with Regard to Personal Data Processing).

[3]The three names that must be mentioned here are those of László Sólyom, the president of the first Hungarian constitutional court, Iván Székely, and Pál Könyves-Tóth.

[4]As we will see later, the Czechs consider the protection of privacy a top priority. A 1998 poll in Hungary found that 43 percent of Hungarian citizens claimed to have heard of the Bureau of the Data Protection Commissioner. Taken together, the three ombudsmen's office is the third most popular institution in Hungary on a list of 18, ahead of trade unions, churches, and parliament.

[5]Act No 256/1992 on the Protection of Personal Data in Information Systems was promulgated on April 22, 1992, and discontinued in effect as of June 1, 2000.

[6]"Most People Believe that Personal Data Is Misused-Poll" CTK, October 6, cited in Privacy and Human Rights (1999): 63.

[7]Act 52 of 3 February 1998, on the Protection of Personal Data in Information Systems in the Slovak Republic. The act superseded Act 256 on Data Protection, enacted in 1992 by what was then still Czechoslovakia, and entered into force on 1 March 1998.

[8]Art. 3: "Data processor means any individual or legal entity processing data on contract with, or by authorization of, a data controller."

[9]The act was adopted in 1997, but it did not become effective until April 30, 1998.

[10]Tax Lax Act No. 137/1997; Police Act No. 30/1990; Insurance Act No. 11/1996; Statistics Act No. 88/1995; Physicians Act No. 28/1996. In March 2000 a bill was put together on electronic signatures, and the Telecommunications Bill reached the parliament floor this past spring.

[11]Reuters, 8 June 2000; Privacy International <www.privacyinternational.org>.

[12]Act No. LXIII of 1992 on the Protection of Personal Data and the Disclosure of Data of Public Interest

[13]This solution originated in Canada and is becoming widespread. The joint protection of data and freedom of information was first introduced in the province of Québec in 1982, which was followed by Ontario, British Columbia, Alberta, and the remaining provinces. In Europe, Hungary has been followed in the adoption of this model by Brandenburg, Berlin, and, most recently, Great Britain. Cf. Comeau (n.d.: 20-21).

[14]DP-FOI Act, §7 (2). Remarkably, the unrestricted use of PINs was first banned by the German Constitutional Court, followed by the constitution of Portugal when the country overcame dictatorship in 1975.

[15]The Hungarian act is occasionally even stricter than the directive. It is far from certain, for instance, that we should keep its application to individuals processing data for their own personal purposes. By contrast, I regard as proved another one of its provisions, which—like Italian law—prescribes application to both the written and the electronic media.

[16]The first three years of the Parliamentary Commissioner for DP-FOI, Budapest 1998, pp. 241-253; website: <www.obh.hu>.

[17]Cf. Recommendation 225/K/1999 in *Annual Report* (1999: 105-111).

[18]There are separate acts to provide for records kept on citizens (66/1992), direct marketing, scientific research, and polls (119/1995), and the handling of personal data in health services (47/1997). Chap-

ters or provisions on data protection are contained in the Police Act (34/1994), the National Security Services Act (125/1995), the Criminal Proceedings Act, the Archives Act (66/1995), the Statistics Act (43/1993), the tax law, and other sectoral legislation. While there are still deficiencies in regulating the Internet, a bill is now being drafted to deal with electronic signatures. In my capacity as DP-FOI commissioner, I have urged the creation of an electronic Freedom of Information Act.

[19]Opinion 6/99, signed by Chairman Peter Hustinx.

[20]After the European Parliament on July 5, 2000, had voted 279 to 259 against the "safe harbor" proposal.

[21]For measuring adequate level of protection, see Raab et al. (n.d.).

[22]In Hungary, the Bureau of the Data Protection Commissioner has operated for five years, creating a public case law of thousands of pages of written documents. See <www.obh.hu>.

References

Annual Report of the Parliamentary Commissioner for DP-FOI. Budapest, 1999 <www.obh.hu>.

Comeau, Paul-André. Annual Report 1999-2000. Abridged version, pp. 20-21.

"Data Protection: Commission Adopts Decisions Recognising Adequacy of Regimes in US, Switzerland and Hungary." Brussels. 27 July 2000.

Millard, Christopher, and Mark Ford. *Data Protection Laws of the World, Poland/18.p.*

Platten, Nick. "Poland Legislates on Data Protection to Pave Its Way for EU Membership." *Privacy Laws and Business.* No. 44 (July 1998).

Privacy and Human Rights, EPIC, Privacy International, 1999.

Raab, Charles D., et al. "Application of a Methodology Designed to Assess the Adequacy of the Level of Protection. . . ." European Commission Tender No. XV/97/18/D.