Hungary

[Privacy in a New Democracy: The Case of Hungary]

Ivan Szekely

Introduction

Constitutional democracy had barely triumphed in Hungary when, in January 1990, the scandal called “Budapest Watergate”, better known to Hungarians as “Duna-gate”, broke out. (Duna is the Hungarian name for the Danube, widely regarded as the great national river of the country.) What happened was that activists belonging to certain new political parties, who used to be called “dissenters” during the not-so-distant days of the overthrown regime, now clandestinely entered the offices of the internal security agencies, and filmed what they found there during the night. The footage presented at a press conference proved that the infamous “III/III Division”, which kept the “internal enemies” of the communist regime under surveillance, had actually survived the symbolic date of the democratic turn (October 23, 1989), and continued tapping the phone lines of new party leaders and activists, keeping their private lives under surveillance and preparing reports on the information thus collected.

Although several commentators later suggested that this was nothing but the aimless and dysfunctional reflex of an apparatus left to its own devices after collapse of the political system that had created and employed it, the scandal was hyped up by the printed and electronic media, which contributed in good measure to the devastating defeat of the surviving reform-communist party in the free elections that took place a few months later. (The surviving reform-communist party received only 10 percent of the votes, the new democratic parties about 90 percent.)

Two weeks after the scandal erupted, the sources also revealed the identity of the person who had helped the documentary crew (named "Black Box") to enter the premises and shoot their film. This was a renegade intelligence officer named Végvári who, after much self-torture, had made contact with the new democratic forces himself, and ended up in front of the television cameras making a public confession.

Duna-gate had more than mere political significance. It triggered a crisis of conscience among rank-and-file agents and their “recruited” civilian collaborators, who often wrote secret reports on their colleagues, neighbors, and even their own families. By drawing public
attention to secret surveillance methods, it also served to heighten public awareness of the vulnerability of privacy in general.

Fig. 1
Hungary beyond the Iron Curtain

Today, Hungary is one of the so-called new European democracies, a member of the European Union, a forerunner of institutionalizing informational rights in its region. The country inherited its central population registration system from the old regime, under which every citizen’s basic identification data, such as name, mother’s maiden name, or date and place of birth, are registered, and this registry serves as an authentic data source for all sectors of public administration. However, the universal personal identification number has been split into three sectoral ID codes used in public administration. The biggest collectors of personal data are the tax authorities, the social insurance and the central voters’ registry of the Ministry of the Interior. Other major centralized data controlling systems include the Central Statistical Office, the central vehicle registry containing both vehicles’ and owners’ data, and the system of employment offices.

With the introduction of a market economy, new private data monopolies have emerged, including commercial banks, insurance companies and private pension funds. Direct marketing is legal and regulated by law; spamming is unlawful but wide-spread. Still, more
than fifteen years after the Duna-gate scandal, accusations and public revelations about collaboration by public figures with the former secret services remain on the agenda.

When totalitarian rule was finally overthrown, the demands and opportunities for reform were quickly exploited. A tightly-knit system of institutional safeguards for the new informational rights was constructed, including the protection of information privacy and freedom of information. As a result, in the late 1990’s Hungary was catapulted into the position of a sort of role model for the fledgling democracies of the region.

The new Constitution includes the right to protection of personal data among the basic rights and freedoms. This provision is expounded by the Constitutional Court, and accordingly reflected in the legal regime, as the right to “informational self-determination” – that is to say, the fundamental principle is that everybody has the right to control the flow of his or her personal data. The legislation follows the European general Act – sectoral Acts model. The basic law (the general Act in this respect) is the combined data protection and freedom of information Act of 1992 (DP&FOIA) which encompasses both the public and private sectors, in terms of all data processing operations, whether digital or conventional, paper-based. The sectoral Acts dealing with data protection (more precisely: with the processing of personal data) include the Records Act, the Direct Marketing Act, the Medical Data Act. Further central privacy provisions are to be found for example in the Police Act, the National Security Act, the Banking Act, the Insurance Act and several other Acts. Today, Hungary has nearly 1000 Acts and regulations that contain such provisions, more than 150 of them explicitly citing the DP&FOIA.

The independent supervisory institution of the new informational rights is the Parliamentary Commissioner for Data Protection and Freedom of Information (often referred to as the data protection ombudsman). His tasks involve the monitoring of the implementation and enforcement of the protection of personal data and the disclosure of data of public interest; investigating complaints and making recommendations (with binding force). The Commissioner’s office has about 45 staff members, and it has a far-ranging investigative license; most of the employees are legal experts or information specialists. His powers encompass both the public and the private sector and are subject to very few restrictions.

Although the Commissioner’s activities have, in practice, little administrative force, most of his positions are issued as non-binding recommendations, the institution is regarded as highly successful, relying on a broad base of professional and public recognition. Most observers feel it has won deference and support for its recommendations among data processors and data subjects alike. At the level of individual organizations the supervision of fair processing of personal data is supported by the system of internal data protection officers and internal data protection regulations, both stipulated by laws affecting a wide range of data processors.

Today, the exigencies and prospects of revolutionary change in guaranteeing personal freedoms and autonomy have lost much of their momentum and currency. In the first few years of the new millennium, international events and domestic developments such as anti-terrorist measures or merging of business databases created unfavorable conditions for the
enforcement of informational rights in Hungary. That said, the country continues to be recognized internationally as being at the forefront of institutionalized privacy protection, which remains a cornerstone of Hungarian democracy. Indeed, Hungary has become something of a testing ground for latter-day democratic states to work out their own privacy concerns.

Fig. 2
Hungary within the EU borders since 2004

I. Key developments in privacy protection - a brief history

Prior to World War II – and, for different reasons, for a long period after it – Hungary was not in a position to deploy a full catalogue of individual rights, including a modern system of informational rights. However, for the student of legal antecedents, it is important to remember that the authoritative Hungarian textbook of civil rights from the period between the two Wars (Szladits 1941) reflects a positively progressive approach compared to similar western European works of the era.

\[\text{\small \footnote{In January 2007 two new member states, Romania and Bulgaria joined the European Union.}}\]
Privacy in those days was conceived of as part of the larger scheme of protecting individual rights under civil legislation, especially the "inner image" of the person, i.e. the general right to human dignity and personality. Equally remarkable in this regard is Hungary's Penal Code of 1878, the so-called Csemegi Codex (Act No. V of 1878), which remained in force throughout the first half of the century, and defined a number of punishable felonies. Among these was the "prohibited revelation of a secret," a notion used to prevent the unauthorized release of confidential information about clients by doctors, lawyers, and other professionals.

The first meaningful step along the road toward modern privacy protection in Hungary was a measure incorporated in the Civil Code in 1977; this declared that “the processing of data by computerized means shall not violate individual rights.” The enactment of this provision was not preceded by any sort of political debate or social interest, nor by any high-profile case surrounded by public controversy. In all likelihood, it emerged from professional circles familiar with western legislation, disputes, and initiatives.

International documents on data protection framed in the early1980s – such as the OECD guidelines and the data protection convention of the Council of Europe – did not pass unnoticed in Hungary. They may have contributed to the decision of the president of the John von Neumann Society of Computer Science in 1981 to propose an “Information Technology Act,” which was sadly deemed “inopportune” by the political leadership at the time.

**A new concept in an old setting**

The first really substantial step – and one that remains seminal today – was taken by an informal multidisciplinary group that had grown up under the wing of KSH, the Central Statistical Office, in the 1980s. This was the last decade of the Kádár Era, named after János Kádár, who came to power as leader of the communist party after the suppression of the Revolution of 1956, and ruled the country for over three decades. The KSH group collected and analyzed western debates, publications, laws, and legal practice, notably including international documents and initiatives pertaining to the protection of personal data and freedom of information.

The group fashioned a comprehensive concept for the information regime of the new Hungary to come, at a time when the country was still being run by the single-party state. The basis of this concept was the dichotomy of a transparent, accountable State and the autonomous, self-determining citizen. In fact, the group prepared two versions of a bill that combined elements protecting both information privacy and freedom of information. One of these two early drafts ultimately became the foundation of Hungary’s combined data protection and freedom of information Act (DP&FOIA), the basic information law still in force today.

Thus by the time communist rule was finally overthrown, not only a general legal concept, but also the single most important constitutional draft incorporating it already existed. This gave Hungary a professional and historical edge during the upheaval of the political
transformation, allowing for speedy completion of the infrastructure of information law and its reinforcement by the appropriate institutions. Most important among these was the office of the Parliamentary Commissioner for Data Protection and Freedom of Information (DP&FOI) Commissioner.

Beyond its professional input, the KSH group later gave Hungary, among others, the first president of its new Constitutional Court, who also became President of the Republic in July 2005; the first and the current DP&FOI Commissioners; one of the professional leaders of a reformed Ministry of Justice; and the author of this study. Those members of the group who did not take up office in the institutions of the new political arrangement founded a civil organization, InfoFilia, the Hungarian Data Protection and Freedom of Information Foundation. During the period until the election of the first DP&FOI Commissioner, InfoFilia was instrumental in promoting up-to-date awareness by translating and publishing major international documents dealing with informational rights.

**The democratic turn and the period of transition**

In October 1989, after long months of demonstrations and tense negotiations, the new democratic forces took over political power, and, on the anniversary of the bloodily suppressed 1956 revolution – the first nation-wide uprising against Soviet rule – the Third Hungarian Republic was proclaimed. This act was emblematic of the single decisive development in recent Hungarian history: the basic transformation of the political system. This transformation went hand in hand with the weakening and eventual collapse of Soviet military and political power, the dissolution of the single party state, the overhaul of the legal system and public administration, the rapid rise of a market economy, the emergence of major organizations in the private sector, the appearance of NGOs, and of course the influence of all of these factors on society. These circumstances created a once-in-a-lifetime chance – a window of historic opportunity that remained open for a couple of years – to shape power relations pertaining to information almost at will, draft the new rights and set up the new institutions, as well as to proclaim information principles and situate them on a reshuffled list of priorities.

Thanks to the efforts of the KSH group, Hungary succeeded in exploiting this opportunity efficaciously and in time, putting in place all the major legal and institutional guarantees before the first wave of change subsided. In the domain of informational rights, this wave came in the form of reforms and initiatives launched from above – in hindsight, one might say it was an elitist movement in its origins.

This is not to say that the masses went unheard in this era. In fact, these voices were very strong, if not in the defense of privacy in particular, at least in their demands for rights and liberties in general. The privacy-related topic that received the greatest social and media exposure was the operation and eventual disbanding of the secret intelligence agency – the Hungarian equivalent of the Russian KGB or the East German Stasi. The single-party state maintained this organization throughout its existence under names, including the “III/III Division”. It differed little from its counterparts in Hungary’s allies, its main function being to
monitor large chunks of its people’s private lives. Although the number of agents and their collaborators and the scope of their activities was never as extensive as in the GDR, everyone was aware of its machinations. This awareness left an indelible stamp on people’s conduct, distorting behavior patterns even in the private sphere – in particular among the dissenters and detractors of the system themselves.

The Duna-gate scandal triggered a broad-based push to unveil the operations of the III/III Division and to enable surveillance victims to access the files it had compiled on them. These demands threw into relief the two poles of classic privacy protection: the omnipotent state and the helpless citizen. Additionally, the institutionalization of privacy protection became inextricably intertwined with the codification of another fundamental informational right, freedom of information – or, as it is often referred to in Hungarian laws, “access to data of public interest.”

It also became clear, as soon as the party-state regime was overthrown, that Hungary’s institutional privacy protection would embrace the European approach. Particularly influential was the German model, in which the right to human dignity is one of the most solid cornerstones of constitutional democracy. Another development emerging from the fall of the old systems was the tendency for individual rights to become not only the subject of political debate, but also the subject of political negotiation and infighting. This made the implementation of new rights contingent upon current political realities and, in so doing, eroded the fundamental value of individual rights, including the right to privacy.

**New rights, new institutions**

Hungary’s new Constitution came into force on October 23, 1989. In reality, however, Hungary did not adopt a new Constitution in 1989 and has not done so since then. Instead, it has radically reworked and repeatedly amended the “communist constitution,” also known as Act XX of 1949. By insisting on thorough revision as opposed to all-out abolition, Hungary demonstrated its commitment to legal continuity and the achievements of the “constitutional revolution,” but it also passed up for good the historic chance to enact a brand new Constitution. Once the elation of transforming the political system had subsided, professional concerns and party politics made it impossible to indulge in such a lofty, symbolic gesture.

The new provisions of the Constitution declare that “everyone in the Republic of Hungary has the right to [...] the privacy of his home and the protection of secrecy in private affairs and personal data” and that “everyone in the Republic of Hungary has the right to [...] access and distribute information of public interest.” The Constitution also stipulates that the guarantees for these two rights have to be regulated by an Act of Parliament, passed strictly by a two-thirds majority vote. As another key measure, the Constitution not only established the institution of the Commissioner for Civil Rights as a pillar of constitutional democracy, but also empowered Parliament “to elect special ombudsmen for the protection of individual [meaning specific] constitutional rights.” It was on the grounds of this provision that a Data Protection and Freedom of Information (DP&FOI) Commissioner was later elected.
April 1991 proved to be a milestone for privacy protection in Hungary, in terms of legal foundations and public awareness. This was when the Constitutional Court passed its Resolution 15/1991 (IV. 13.) AB, ruling unconstitutional the universal and standardized personal identification number devised for unrestricted use. With “the Court banning the ID number,” as the man of the street put it, Hungary became part of the group of former dictatorships that considered all-purpose centralized files on citizens irreconcilable with the principles of constitutional democracy. This camp includes Portugal, which enshrined such a ban in its constitution as early as 1976. In Hungary, the old regime had used a universal code to tag citizens from the 1970’s onwards. During the period of democratic transition, both the personal ID number and the State Population Registration Office that kept it on file became emblematic of the single-party state.

Social awareness to the ID code affair, and privacy issues in general, owed much to this Constitutional Court ruling, which provoked fierce criticism among the entire government apparatus. Some detractors warned of nothing less than the end of viable state administration, while others took issue with the unreasonable costs of switching to a new, decentralized records scheme. These officials gave dire warnings of chaos in the offices and impossible budgetary demands. Now it has become evident that these fears and counter-arguments were unfounded.

However, the abolition of the universal ID code was not the only feature of this well-known Resolution. In addition, the Resolution threw out the entire system of population registration, mandated the legislature to enact a law on the protection of personal data and the disclosure of data of public interest, and to concretize its general principles in a series of sector-specific acts. Most influentially of all, the Constitutional Court outlined a thorough theoretical and technical interpretation of the right to protection of personal data, defining it as the individual's right to make active decisions about information that concerns him or her, rather than merely as the passive right to have such information protected, as in the traditional sense. In other words, citizens are no longer defenseless individuals who, if they behave themselves, deserve the benevolent protection of a paternalistic state. Instead, they are autonomous people with free will who are entitled to determine for themselves who can use information about them--and for what purposes, under what circumstances.

**New laws, new regulations**

The key Hungarian privacy law – an act combining elements of both data protection and freedom of information (DP&FOIA) – was passed in the fall of 1992, following lengthy debate in professional and political circles. Thanks to the conscientious groundwork that had preceded it, the National Assembly adopted the DP&FOIA without a single contrary vote. The idea of enacting a single act providing for both informational rights was inspired partly by the Canadian model, and partly also by widespread desire to legislate safeguards for both rights simultaneously.

The joint regulation sought to prevent any easy way of pitting the two rights against one another in an effort to play privacy off against freedom of information, or vice versa.
Nevertheless, there have been abuses since the DP&FOIA entered into force. Some public officials have sought to withhold documents from applicants on the grounds that these contained their signatures – unquestionably personal data –, and as such warranted their own discretion over disclosure. Obviously such twisted arguments run counter to both the letter and the spirit of the law.

In essence, the DP&FOIA defines personal data and the right to their protection – the latter now interpreted by the Constitutional Court as informational self-determination. It then proceeds to define, as a rule of thumb, all information that is not personal in nature as data of public interest, and therefore subject to public access. This simple model sheds clear light on the original intention behind the law – namely to use both informational rights as means to rein in the excessive informational power of government.

In the area of privacy, the DP&FOIA explicitly prohibits data processing, except with the consent of the data subject, or as required by law, understood narrowly as an Act of Parliament. It spells out the subject’s option of legal remedy, and classifies the act of “unauthorized data processing” as a violation punishable under the Penal Code. The law furthermore establishes the office of the DP&FOI Commissioner, as an independent body in custody of informational rights. Unfortunately, it took Parliament another three years to elect the first DP&FOI Commissioner.

By and large, the law adopted in 1992 was a modern piece of legislation. It inspired a series of legislative efforts in a number of new democracies from the Baltic countries to the successor states of the former Yugoslavia. It rigorously incorporated the major tenets and provisions of European privacy norms. Indeed in some ways it was slightly more stringent than its European counterparts – as in provisions for data transfers abroad. The advocates of stringent and consistent regulation argued – and they continue to insist today – that new rights and liberties needed and warranted stricter protection in former dictatorships than in traditional democracies with true and tried legal and social practice.

The adoption of the DP&FOIA did not mark the end of legislative efforts pertaining to privacy. Starting in the mid-1990’s, a series of sector-specific data protection laws saw the light. Some of these merely serve to expound upon the general rules of the DP&FOIA and apply them to specific areas from the health sector to higher education, while the majority stipulates exceptions. In 1996, Parliament passed the Identification Numbers Act, which complied with the Constitutional Court’s Resolution discussed above. It abolished the universal code, replacing it with three specialized numbers: the personal identification number (its use far more limited than that of its predecessor), the tax identification number, and the social security number.

Beyond proper Acts of Parliament with their own independent titles and numbers, sectoral legislation has prominently included privacy provisions that have been incorporated as chapters, sections, paragraphs and appendices in a number of other laws besides the DP&FOIA. These include, among others, the Anti-Discrimination Act, the Higher Education Act, and the Electronic Commerce Act. In addition, privacy provisions are to be found also in several regulations lower down the hierarchy of statutory instruments, which do not provide
for processing of personal data in and of themselves, but may provide more detailed interpretations of the details of existing Acts of Parliament. The number of laws and decrees with implications for data processing continues to rise. Overall, the constitutional right to the protection of personal data has been successfully integrated with the system of Hungarian law. Yet in its spirit and effect it does not follow the traditional branches of legal hierarchy such as the areas of public and private law, instead it constitutes a new dimension permeating the entire legal corpus.

**The Parliamentary Commissioner as independent supervisor**

One could have predicted that strong political and business interests against guaranteeing information privacy for the citizens of the Third Republic. Accordingly implementation and enforcement of the new informational rights would require an independent supervisory agency. But who could be the most efficient, legitimate and publicly accepted supervisor in the turbulent situation of a new democracy? A civil organization, a popular front committee, a new government agency, or an honorable individual? In the DP&FOI Act of 1992, legislators envisioned the latter: a one-person office of the parliamentary commissioner, an independent institution to monitor informational rights with a special range of tasks.

In 1993, the National Assembly adopted the Act on Parliamentary Commissioners, which defines the functions and procedures of a parliamentary commissioner of the ombudsman type; that is, a state official appointed to provide a check on government activity in the interests of the citizen, and a general deputy, both vested with general powers. This Act upholds the right of Parliament subsequently to elect specialized commissioners to safeguard specific constitutional rights. This latter measure was motivated by the aim of ultimately deploying three commissioners: one with general powers (plus his deputy, actually the fourth commissioner), one for the protection of national and ethnic minority rights, and one for the protection of personal data and freedom of information – whose duties and powers had already been specified by the DP&FOIA.  

In the summer of 1995, a year and a half behind schedule, the National Assembly finally elected its first commissioners. These included the DP&FOI Commissioner, László Majtényi, a professor of law. The powers attributed to the DP&FOI Commissioner are far more extensive in scope than those of his colleagues – mainly because they had been drawn up separately by the DP&FOIA in 1992, one year before the Act on Parliamentary Commissioners.

Although the office had been practically unknown in Hungarian law, it took only a few years to find a proper niche within Hungarian institutions and public consciousness. Lodging a complaint with the DP&FOI Commissioner – essentially an alternative to filing a suit in court – has been a popular option with plaintiffs from the start. It is only rarely that individual data subjects (or the lobby groups behind them) turn to court, most parties preferring a

---

2 In 2007 the Parliament abolished the institution of the Deputy Commissioner and established a new parliamentary commissioner for the protection of environmental rights, called Parliamentary Commissioner for the Future Generations.
submission to the Commissioner. The Commissioner’s case law in Hungarian data protection has come to cover a wide range, from ovum donation to the administration of anonymous HIV tests, and from revelations about citizens’ political pasts to spamming and direct marketing. This body of law has mainly emerged not from courtrooms but from the evolving practice and recommendations of the Commissioner.

Landmark cases

Hungary’s first high-profile privacy controversy was the “lottery jackpot affair.” In October 1995, somebody won the biggest prize in the history of the Hungarian lottery, which had been accumulating for a long time. Szerencsejáték Rt., the State Gambling Company, had the television crew of a news program named “Objektív” and photographers from Népszabadság, one of the largest-circulation dailies, do several “takes” on the “discovery” of the winning ticket. Using the footage, the TV crew managed to identify the name and address of the winners from the reverse of the ticket, and called on the family late at night. Despite the wishes of the winners, who requested anonymity, the interview with them was aired the following day. The imperfect distortion of sound and video, along with the airing of their personal data, made their identity publicly known.

The DP&FOI Commissioner investigated, and ended by condemning Szerencsejáték Rt.’s processing of the data and the TV crew’s conduct. True, the fine print on the back of lottery tickets read, “I consent to the use of my name and address in the news media.” But it was obvious to everyone that the TV crew had physically infringed upon the privacy of a family and – given the huge amount of the prize thus disclosed – had even put their lives at risk by misleading them about the purpose of the interview. Sadly, the TV crew never really admitted their wrongdoing. The case divided the media industry itself, with some journalists arguing that alert TV journalists had all the right in the world to delve into private events of interest to viewers.

In 1998 a girl of 13 applied for an abortion, with the consent of her mother. Her case, which came to be known as the “Case of the Girl from Dávod”, received wide exposure due to TV coverage and triggered an investigation brought by the Commissioner. This case proved even more divisive, as it forced everyone familiar with it to take a stand on the boundaries of privacy and, by implication, also on questions of ethics and ideology. Having learned of the pregnancy, a family rights advocacy group initiated an official process to stop the abortion, and helped to publicize the case.

The mother lodged a complaint with the Commissioner in order to identify the person guilty of having abused her daughter’s sensitive data. The ripples generated by the case reached both the electronic and printed media. A prime-time report by public television featured the names, address and images of the girl and her mother, and even showed footage of their house and living environment. The abortion which was performed in the meantime rendered the debate between pro-choice activists and their detractors pointless, even as the continued publicity deprived the family of the last vestige of their privacy. Remarkably, the pro-life
commentators never acknowledged the subjects’ right to privacy or the legal provisions governing it as legitimate concerns.

A case known as the “VIP list scandal” triggered social debate over another area of privacy. It centered on Postabank, one of Hungary’s major commercial banks. Postabank offered loans and investment opportunities to certain leading politicians, public officials, and celebrities at much more favorable rates than the prevailing market terms. Having acquired a list of names of parties and the benefits they received, the press assumed that improprieties had occurred. Not only did they hold that the bank had offered preferential treatment in the hope of improving its lobbying positions, they also charged abuse of office by several of the individuals involved.

The Commissioner answered a journalist’s submission by asserting the public release of the personal data in question could not be defended on any legitimate grounds. Nevertheless, he held, there were indeed strong reasons to enact new provisions assigning broader limits of exposure for individuals in public office. In his position statement, the Commissioner cited a number of Resolutions by the Constitutional Court, which established narrower constitutional protections for the privacy of public officials than for that of the ordinary citizen. Ultimately, the Commissioner was unable to prevent the publication of the VIP list, which also featured the data of several individuals without public responsibility, including actors.

After the turn of the millennium, high-profile privacy cases were increasingly filled with political content. In 2001, the so-called “National Image Center,” an agency created during the previous government cycle, illegally obtained from the Ministry of the Interior’s central records the data of at least one person in practically every Hungarian household, and proceeded to mail them issues of the magazine entitled Millenniumi Országjáró [“Millennium Country Rambler”]. The aim was to promote the policies of the conservative government in power.

In response to a barrage of complaints, the Commissioner called on the cabinet members in charge to stop the unlawful circulation of the magazine, but to no avail: the government continued to mail the publication to citizens until it lost the next elections in 2002. Attacks on the government’s abuse of its citizens’ data in a political direct marketing campaign was high on the agenda of the political opposition. Ironically, a year later, the socialist party, which had led the opposition, availed itself of very similar means when it mailed a campaign letter by its candidate for prime minister to addresses processed in violation of the law. (Hungarian laws prohibit political parties from engaging in direct marketing activities. Pursuant to the Election Procedure Act, political parties may not legally acquire citizen addresses until 20 days prior to Election Day.) The Commissioner responded by calling on the party to destroy the list in question. Although the Party Chairman insisted that the party had acted within the law, he destroyed the databases publicly, on the record.

Towards the end of his six-year term in office, the Commissioner issued several recommendations, such as the Millennium Country Rambler case, directly blocking interests of the prevailing power-holders. In reply, certain populist political circles went so far as to
propose abolishing the office of DP&FOI Commissioner altogether. Even the more sober voices within government made it clear they would not support the reelection of the country’s first Commissioner for another term, despite his uncontested qualities as an individual and professional.

Though no political formation of any standing had the slightest intention of getting rid of the institution itself, the election of a new Commissioner turned out to be far more difficult than anticipated. The few individuals who met professional eligibility requirements and proved acceptable to both major political coalitions declined the candidacy, while candidates nominated by one side were consistently voted down by the other. Finally, after negotiations lasting almost six months, the National Assembly succeeded in electing the country’s new DP&FOI Commissioner, Attila Péterfalvi, a lawyer from the first Commissioner’s office. During the transition, the General Commissioner – one of the three parliamentary commissioners – filled in for the DP&FOI Commissioner, running the Office and issuing recommendations and position statements on his behalf. This solution is obviously subject to all sorts of criticism on both legal and professional grounds.3

The case spurring the greatest debate since the second Commissioner took office broke out around the website Hálapénz.hu in 2004. (Hálapénz in Hungarian means an informal payment or gratuity given to doctors and health care workers.) Operated by private individuals, the site featured “a searchable nationwide database of obstetricians” from which the user could access patient evaluations and learn the amount of the informal payment expected by each physician for care supposedly financed in full by social security – hence theoretically free of charge to the patients. Visitors typically accessed the site to learn how much it would cost them to give birth under the supervision of a specific obstetrician, and precisely what services they could expect in return.

It was of course the online posting of this latter information that stirred heated professional and social debate. Most commentators agreed that gratuities in health care were socially detrimental, but the controversy was about more than just the legitimacy of this custom. The advocates of disclosure proposed that the freedom of communication and opinion entitled expectant mothers and their relatives to share their experiences with obstetricians online. They argued that, in conducting childbirths financed by social security, doctors used public funds and fulfilled a public function – and that therefore their data relevant to these activities did not merit protection under privacy regulations. As for patients referred to a “private practice,” they typically received care using institutions and equipment financed by public funds as well. By contrast, the proponents of privacy stressed their perception of the doctor-patient relationship as a strictly confidential one, adding that the physicians involved had never abused their office. According to their view individuals who did not offer a gratuity received equally conscientious care, and gratuities were normally expected only for certain extra services, such as the obstetrician personally attending and conducting the childbirth

3 At the time of writing a similar situation occurred: in December 2007 the Parliament failed to re-elect the DP&FOI Commissioner in office, therefore in the interim period the new General Commissioner – a newcomer himself in the office – had to fill in for his fellow commissioner. The new candidate was again rejected by the Parliament in February 2008.
even when off duty. The DP&FOI Commissioner came out in support of this latter opinion. As a result, the operator removed the site from the Web.

**Underlying processes and international influences**

The legal history and the landmark cases do not necessarily reveal those background forces, both internal and external, which ultimately exert a fundamental influence on the direction of progress. As to the internal forces, during the period following the radical transformation of the political system in Hungary, the three changes with the most notable consequences were: the reform of the state’s mechanism for handling information, the emergence of a new data processing monopoly, and the modernization of the relevant technologies.

The first change came together with the establishing of institutions and tools for steering, supervising and balancing state administration that characterize modern constitutional democracies; consequently, there have been changes in the ways these new institutions demanded information and linked their databases. This is not to say that the thirst of government for ever larger doses of information has been quenched. On the contrary: renewed efforts at centralization have signaled a call to link databases more intimately than ever before, and resulted in the elaboration and promotion of a new system of efficiency-based arguments such as the necessity of avoiding parallel data registration.

The second is the emergence of large data processing organizations in the private sector, such as commercial banks, insurance companies, private pension funds and direct marketing firms, mostly subsidiaries of multinational companies – some of them handling personal data of almost one third of the population of the country – supplanting the government’s former monopoly on information. Growing up around the Big Brother, these “Little Brothers” claimed their share of informational power, and have continued to exercise that power over large masses of data subjects. These organizations, for example – borrowing the techniques from their western parent companies – are secretly monitoring people’s buying and surfing habits on the internet and use this information for offering products and services with unfair “dynamic pricing”, in other words, showing a higher price than advertised, to those supposed to accept it.

The third major change involves more than just replacing computers, in both the public and the newly reborn private sector. It also meant introducing qualitatively new methods of keeping and analyzing records, such as the building of “data warehouses” and performing “data mining” analyses, as well as the linking of personal data systems that had so far been handled separately. As a result, banks can share with each other data relating to bad debtors, or advertising companies can flood potential customers with unwanted emails based on their consumer profiles.

In this way, the power to collect and analyze information that so deeply influences the life of the individual was not really reduced in the newly democratic Hungary, so much as restructured and rendered more transparent, as well as being made subject to more extensive safeguards designed to protect the individuals.
Shaping privacy protection in Hungary has been the considerable weight of the OECD Data Protection Guidelines, the Council of Europe Data Protection Convention, and the EU Data Protection Directive. Hungary became a member of the OECD in 1996. Compliance with the Guidelines has not posed any difficulties since the adoption of the DP&FOIA, considering that the concept for the Hungarian legislation had been well harmonized with the Data Protection Principles since the days before the democratic turn.

The Council of Europe granted membership to Hungary in 1990. Although the country had signed the Convention in 1993, somewhat surprisingly it did not ratify or promulgate it until 1997 and 1998, respectively. The Ministry of Justice explained the delay by saying that they did not want to ratify the Convention until the appropriate regulations for the data processing sectors identified by the Council of Europe Recommendation had been implemented. In this way, the Council of Europe norms left an indelible stamp on the development of Hungarian data protection laws. At the same time, forces intent on limiting data protection, such as the police and other law enforcement agencies have also been very active in exploiting international relations. A case in point was the 2001 Convention on Cybercrime, a legal document containing several provisions overriding national data protection laws, which happened to be opened for signatures in Budapest.

Hungary joined the European Union in May 2004, during the latest wave of EU expansion, when the number of members grew from 15 to 25. Concurrently, of course, Hungary had to fall into line with the direct and indirect regulatory institutions of the EU, including its Directives. This is why the accession had been preceded by a lengthy process of legal harmonization. Meeting the requisites of the Data Protection Directive did not demand any major amendments in Hungarian law, because the competent EU body had already recognized Hungary – at her own request – as a country offering an adequate level of data protection. Hungary had in 2000 become the second non-EU country after Switzerland to secure this recognition. The result was to ensure that it would receive essentially the same treatment as any EU member state regarding the cross-border transfer of personal data, and that Hungarian citizens would be entitled to the same degree of protection of their personal data as any EU citizen. To bring about full legal harmony it was still necessary to broaden the powers of the DP&FOI Commissioner, which the National Assembly duly accomplished by amending the DP&FOIA in 2004.

Despite harmonization efforts, the new international relations and commitments have had a rather contradictory impact on the fate of informational rights, not only in Hungary but in other countries of the region as well. On the one hand, the international community expects the new democracies to enact laws guaranteeing individual rights and liberties. On the other hand, various other factors have put pressure on these countries’ privacy guarantees. These include their fresh membership in NATO; the demand to join the common European policy on external border controls and sharing of travelers’ data, the so-called Schengen Region, and the consequent broadening of their responsibilities in guarding borders and cooperating with Europol and other international investigative agencies; and even their informational dependence on US support in areas of trade, investments, technology transfer, or immigration. External demands for excessive processing personal data, such as the retention
of data of mobile telephone calls, for giving freer rein to secrecy legislation – for example, introducing the four-level classification of "cosmic top secret", "top secret", "secret" and "confidential" types of documents restricted from public access –, and collaborating on anti-terrorism measures have had adverse effects and led inevitably to restrictions on informational rights, no matter how recently the latter may have been enacted.

II. Public Opinion

The first comprehensive public opinion survey on privacy issues in Hungary was conducted in 1989-90 by the Hungarian Institute of Public Opinion Research (MKI). Conducted in the midst of the political transformation, it served to provide a snapshot of views and attitudes in flux. But the results also pointed to several themes in public opinion that are presumably less prone to fluctuation or change (Székely et al. 1991).

Using a representative sample of 1000 individuals, respondents were asked: "Would you personally object or not object if the following data about you were made publicly available?" The survey concluded that the most sensitive personal data in Hungarian population were those pertaining to family, financial status, and health, with every other respondent objecting to the disclosure of such information. (Fig 3, dark columns) The least sensitive category comprised information related to ethnic background, level of education, and occupation. The universal personal ID code, still in use in those days, ended up in mid-field.

![Data sensitivity](image)

Fig. 3

The survey also included questions about examples of invasion of privacy: "Is your private life invaded or not invaded if someone taps your phone?", etc. According to the responses, the most sensitive examples were: letters received open (over 90% of the respondents objected it), conversations and telephone calls monitored. (Fig 4, dark columns)
The survey also showed that although Hungarians had a moderate awareness of the potential uses and abuses of their data, nearly all reported themselves to be obedient suppliers of their own personal information, whether it was sought on a mandatory or voluntary basis. Responding to the question: “Does it happen or not happen that at official places you refuse to give certain data about yourself?”, only a very few cases of refusal to disclose personal data were reported. However, the respondents’ answers revealed a considerable degree of distrust toward power and control over information, along with its beneficiaries and practitioners.\footnote{A comprehensive international survey on the globalization of personal data, conducted in 2006 at Queen’s University, Kingston, Canada, showed an increase in acceptance of all major data processing techniques and a decrease in the level of distrust and resistance in Hungarian population (Székely, forthcoming).} Given that informational privileges in Hungary at the time of the survey were predominantly held by institutions of the single-party state, state-owned corporations, and personnel departments, the most obvious targets of distrust were government agencies in general, and also computerized records as such.

Respondents took the most positive view of data practices at the workplace and those of OTP, the National Savings Bank that was still a monopoly in those days. By contrast, personal data use by the tax authorities and utility bill collectors elicited the strongest dislike among citizens.

Perhaps the most remarkable result of the survey was the discovery of a “mysterious”, privacy-conscious social stratum. Sixteen percent of the respondents were significantly more sensitive to transgressions of their information-related privacy, in all aspects touched upon by the survey, than the rest of the population (Figs 3 and 4, light columns). Interestingly, however, no difference could be detected between this subset and the entire sample at all in terms of social status – such as age, sex, level of formal education, or place of residence –
or political affiliation that could have correlated with the discrepancy. This suggests that the demand for informational self-determination does not follow precisely understood social roles but represents a rather special dimension.

Quite noticeably, even without a poll, awareness of the DP&FOI Commissioner’s role has been a major factor behind the currency of privacy as a topic in public discourse. In order to ascertain political and public acceptance, in 1998 the three parliamentary commissioners ordered a poll. That survey found the three commissions together to be one of the most popular public institutions, preceded only by the President of the Republic, the Constitutional Court, and the political party preferred by the respondent. According to the representative survey, 43% of Hungarians claimed to have heard about the DP&FOI Commissioner three years after the institution was created.

**Public opinion and the media**

In 1991, MKI conducted another comprehensive survey, entitled “Aspects of Privacy and Informational Autonomy in the Press,” a review of articles from four national dailies from 1987 to 1990. The researchers collected what they hoped was an exhaustive list of publications and analyzed their content, in particular the ways in which they construed privacy-related. The aim was to examine the representation of informational privacy in the leading press organs during the period of democratic transition.

Despite the relatively large number of articles devoted to privacy-related issues, the quantitative and qualitative analyses revealed that the topic itself did not get the attention of the press that it deserved. Even though the politicization of informational rights pushed these news and stories briefly into the limelight, later it was the same process of excessive politicization that led both the media and the public to concentrate too much on one, relatively minor, aspect of the problem. The case that provoked the most vocal response in the press of the day was Duna-gate and the associated surveillance scandals that we have already discussed. However, even these articles failed to address the essential fact that the victims were subjected to illegitimate surveillance of their lives, professional and personal relationships, and even their bedroom secrets, as private individuals. Instead, the focus was always on their status as politicians in opposition.

Since those days, and particularly since the election of the DP&FOI Commissioner, the media has shown much more interest in the topic. And yet, the over-politicized nature of the issue – that is, everything must be evaluated in the light of party politics – has remained with us as one of the most stubborn evils, a sort of morbus hungaricus, or Hungarian disease, that keeps haunting not only the media but public affairs in general as well.

**Professional reception**

There are several professional groups with vested interests in the broadest possible access to the data of clients, existing or targeted. The representatives of government offices and
business ventures are obviously biased in their assessment of privacy concerns by their professional and business interests, for example in selling and buying marketing lists from the central population registry. Ironically, senior public officials and entrepreneurs with a tendency to scorn advocates of privacy often take the opposite view as private individuals. They object to being subjected to the very same methods and techniques by which they themselves seek to encroach on the privacy of others, and for the use of which they seek to win legitimacy by public consensus. An executive director who aggressively propagates the use of consumer profiles, would not be happy if someone built and used his or her own profile. We find, however, two disciplines where any business interest is certainly out of the question: those of law, and of information science. Both of these have a decisive say in assigning limits to the precedence of informational privacy.

In Hungary, civil lawyers, those most engaged in data protection issues, consider the Civil Code as their fundamental source of law, a veritable Bible that guides their views of data protection. Yet Hungarian data protection law derives from a constitutional right, and as such stretches across all the traditional elements of the legal corpus. Many Hungarian lawyers still find it difficult to reconcile the two approaches and the practical consequences they entail. Those lawyers who work in a sector with vested interests in evading privacy typically identify with the standpoint of the company or industry in which they make their living. As a result, the promotion of data protection and informational privacy in professional and public circles has become the privilege of constitutional lawyers, a peculiar elite in the legal sector; indeed data protection itself has become something of an elitist subject as a result.

As for those who work in the IT sector as system designers, programmers or operators, the hostility and lack of comprehension that often manifests itself on the surface is usually underlain by a tendency that is not unique to Hungary but can be found in many countries boasting a highly advanced ICT. This is because, as a rule of thumb, the IT professional is always a natural ally of the more powerful party in the equation (that is, the government agency or the business company rather than the citizen or the customer), which commissions his services, pays him, and presents itself as the underwriter of his professional career. In terms of informational privacy, this stronger party is invariably the data controller, understood as a public or private-sector organization responsible for and interested in processing the data of clients, prospective or existing, as well as of ordinary citizens and those registered to vote. To become a chief information officer of a data handling monopoly such as a big insurance company is always more appealing for these professionals than working for a grass-root civil organization.

The author’s experience, both as a consultant and as a professor teaching future IT professionals, suggests that an average system developed by IT personnel is bound to reflect the perspective of the data controller, with little if any regard for the interests and rights of data subjects. The information technology specialists take “Big is Beautiful” as their motto. They think in terms of designing, implementing, operating and linking large systems in which personal data are collected, processed and analyzed in ways beyond the control of data subjects and supervising authorities. To be sure, there are also IT professionals in
Hungary who dedicate at least part of their talent and efforts to the benefit of the weaker side. This small non-conformist minority, often is often ostracized as “a bunch of hackers.”

Let me mention one last trait that characterizes the IT attitude: Many computer professionals are steadfast in equating data protection with data security. This globally familiar misconception no doubt has more widespread and deeper roots in Hungary and other post-communist countries with a history of authoritarian rule. For here, no other interpretation was possible before the democratic transformation: since data protection serves the interests of the individual, while data security mostly serves the interests of the data controller or the informational power, data security proved to be a perfect fit for the ideology of the totalitarian state and its organs.

**Attitudes of civic associations**

NGOs represent special voices on privacy in the public forum – voices that are frail in absolute force but of quite radical in their claims. The small number and belated formation of civilian organizations concerned with informational rights seem to reflect an empirical correlation noted in a number of new European democracies: where there is an official custodian in place, the civilian push for informational rights will be weak; conversely, where official supervision is inefficient or nonexistent, NGOs will undertake the missing function of enforcement on their own.

In Hungary, the wide recognition of the DP&FOI Commissioner as the custodian of information privacy and access to public information, along with reforms trickling down from above, has helped to shift the focus of civilian activism to other areas. These include environmental protection, help for the homeless, and the fight against gender discrimination. In other countries of the region, such as Bulgaria, the missing institutional protection of informational rights has triggered grass-roots privacy activism.

Most of the few Hungarian civic organizations focusing on informational rights have emerged since the turn of the millennium. One that had existed before the foundation of the DP&FOI Commission (and which still exists) is the Hungarian Civil Liberties Union, whose core activity is providing public advocacy and free legal aid in connection with personal data protection. More recently, a new wave of concern has brought us Technology for the People (TEA), and the No Camera Group. All of them are composed of a handful of dedicated professionals and activists who are able to organize public events and attract the attention of the media.

A case in point was a flurry of NGO activity against video surveillance of public areas. This was provoked in no small part by the Commissioner’s ambivalent position on the issue, which led him so far as to install CCTV cameras in his own office building. The No Camera Group organized street performances, set up symbolic changing booths in front of public surveillance cameras, and performed strip-teases and changes of clothes amidst the crowds of downtown Budapest. Their civil disobedience over informational privacy principles are enforced and over the operation of the institution appointed to their protection.
Since 2001, the annual presentation of the Hungarian Big Brother Awards – the local version of the negative prize invented by Privacy International that has been adopted in several countries – has been a popular manifestation of radical civilian censure. TEA organizes this event, and a panel of respected personalities assigns the awards, which are handed out before a small audience – but always with the media in attendance. Ironically, the most intense controversy has surrounded the person of the Commissioner himself. In 2002, he was among those nominated for the Big Brother Award, on account of the cameras installed on his official premises. In 2004, he received another nomination – anyone may anonymously nominate individuals through the internet for the first round – this time for his lenient position on cameras installed in department store fitting rooms. In this case, the Commissioner found himself among the finalists and, after the online votes given to the finalists had been counted, actually ended up receiving the Audience Award. Attila Péterfalvi, the second DP&FOI Commissioner in office, not only appeared at the awards ceremony, but – unlike other recipients to date – accepted the award, although he made a point of voicing his disagreement with the rationale for his own selection.

III. National Culture and Traditions

Before the fall of the one-party system and the political transformation, there was obviously no real possibility for public debate about privacy and the right to a private life. In other words, these issues had not been properly thematized or made available for systematic study and research. Under the circumstances, one might perceive an element of surprise in the way – always committed and optimistic but never unrealistic – in which the first DP&FOI Commissioner assessed the situation in his first Report to Parliament, on the years 1995–1996, as follows:

“The sensitivity of Hungarian society to data protection, and the right to informational self-determination is more advanced than was previously anticipated. Data protection does not represent a luxury demand of people of higher social standing or educational level, and the sensitivity to data protection cannot be closely attributed to social standing: It spreads across Hungarian society from the unemployed homeless to the highest ranking citizens.” […]”The personal identification number and the problems of shared registrations demanded considerable efforts from the office. Apart from the »data protection related to the change of the system« […] the other classical fields of data protection are equally apparent in the Office’s caseload.”

At the same time, the Commissioner found that “Society’s general antipathy towards and distrust of the State is also remarkably strong” and that “The process of change within the political system does not seem to have come to an end in respect of social or legal values.” (Majtényi 1998, pp. 11–12) These words were formulated a few years after the “constitutional revolution”, the peaceful handover of power to the new democratic forces.

While there was no disputing the benefits of the bloodless collapse of the past political regime and the measured pace of legal and institutional reform, they clearly amounted to
passing up more than one cathartic and symbolic moment of opportunity to close the afterlife of communism and to open up the files of the past regime. In vain had the Duna-gate scandal broken out, the perpetuated ban on accessing secret service files left the government vulnerable to blackmail, accusing high ranking officials of being a former agent. On the part of the surveillance victims, the archives became targets of endemic distrust and discontent, being accused of hiding compromising documents in order to protect former agents.

But not all of the political forces active under the new democratic rules embraced informational rights whole-heartedly. The initiative mentioned above, aiming at nothing less than the abolition of the entire data protection apparatus, won influential supporters. One of these figures declared that “data protection is alien to the Hungarian popular spirit” (István Csurka, leader of the far-right Hungarian Justice and Life Party, around the turn of the millennium)

Among the symptoms of a new capitalism springing up without appropriate checks and balances we find notoriously dismal standards of business ethics. These have allowed large multinational companies in Hungary, as in other recent democracies, to subject their clients and employees to treatment, including the use of their personal data, that they would never get away with in their own countries. In a big shopping mall in the neighboring Czech Republic, for example, the female cashiers were allowed to spend only a limited amount of time in the restroom, just a few minutes each workday. Cashiers who were menstruating were marked with a red ribbon and allowed to spend a few more minutes daily in the restroom. As a result, everybody in the shopping mall, including supervisors, male and female employees and shoppers were visually informed about this sensitive personal data of the cashiers. This practice, which had not been introduced in the company’s Hungarian shopping malls, due to adverse publicity, was not only unlawful but humiliating.

The general public concerning privacy matters has been evident not only toward government but also toward the business. There is a widespread and stereotypical belief along the lines of “You can only get rich if you break the law” or “The wealthy always have something to hide.” All this goes hand in hand with a hyped-up consumerism relying on a customer base too gullible and inexperienced to see a commercial offer for what it is. This is why the majority of marketing techniques continue to work in Hungary. The average consumer seems willing to go along with any scheme, including requests for his personal data – even while he or she remains skeptical of the honesty of business intentions by and large.

**IV. Winners and Losers**

The institutionalization of the right to privacy, along with other far-reaching changes restructured informational power relations in Hungary.

During the period characterized by the establishment and consolidation of fundamental rights and their institutions, it was relatively easy to set up typical alliances that exist in other developed countries, with governmental and newly emerged private-sector holders of data
on the one side and committed experts and scholars, the media, and the DP&FOI
Commissioner himself on the other side. It was the latter coalition that proved victorious in
the institutionalization of these rights.

Large private-sector users of personal data, including banks and insurance companies, saw
their informational power restricted in the 1990’s. But they soon found ways to get round
the restrictions by introducing sophisticated data processing technologies such as data
warehouses jointly operated by a group of companies – typically financial holdings –, and by
concealing the true extent and underlying purposes of the processing from both data
subjects and auditors. When faced with criticism, these organizations are quick to deploy
token solutions and empty rhetoric. As for government organizations, they initially seemed to
yield to constitutional demands and partially decentralized their records for a few years
directly following the democratic turn, for example, established independent tax and social
security registration systems. But later they improved their lobbying positions in the
legislation and redoubled their efforts at re-centralizing information.

Contradictions abound in the situation of employees. On the one hand, they belong to the
camp of the winners in a general sense, given that data protection law vests them with a
variety of means to exercise control over the fate of their personal information. In theory,
for example, they can refuse consent to the introduction of new fraud detection systems
based on the analysis of their personal transactions, and they have a right to inspect video
recordings made of them. In addition, restrictions have been placed on the scope of data
processing operations available for the employer (e.g. secret workplace surveillance is
forbidden, data processing must be based either on law or the informed consent of the
employee).

In practice, however, employees must be regarded as losers in the transformation,
particularly in the private sector. There employers have brought about a situation in which
workers fear exercising their rights for fear of losing their jobs or benefits. Moreover, they
often do not learn about the violations of those rights until long after the event. Instrumental
in perpetuating this sorry state of affairs has been the decline of an already discredited trade
union movement and its effective banishment from certain new business sectors. Employees
in hypermarkets or department stores owned by multinational companies sometimes have no
choice but to deny their trade union membership.

In any event, the workplace has become a prolific source of privacy-related problems, from
the monitoring of e-mail correspondence and web surfing habits to tapping phone lines and
even resorting to lie detectors purportedly “based on voluntary consent.” (A comprehensive
catalogue of real-world examples can be found in Szabó and Székely 2005.) In a case taken
up by the Commissioner’s office, a Hungarian company unintentionally replayed in real life
an ironic scene from a film, Egészséges erotik ak (Healthy Eroticism), parodying the
Communist Little Brothers who were watching the female employees’ changing-room
through secret video cameras – the real-world company had installed similar cameras in
these changing-rooms “for security reasons”.

23
There is one group that always sides with the winners: those who design and operate systems for the filing and handling of personal data. They are the natural allies of data controllers. Even an information technologist working in the Commissioner’s office said recently during a professional meeting: “Climbing Rose Hill in Budapest ten times cannot compare with the glory of climbing Mount Everest once” – meaning that creating big data systems is always more attractive for the IT professional than playing with small, interoperable, although more privacy-friendly systems.

On the whole, the media are clearly to be grouped with the winners of the transformation. But they have had to learn not just how far they may, and indeed must, go in uncovering the secrets of the state, but also where the limits lie to their passion for divulging the private secrets of citizens.

The institution of the DP&FOI Commission in Hungary has been an undoubted success. Indeed, it has proved to be the single most effective tool for protecting constitutional rights. Recently it has received administrative-type powers in compliance with EU norms. But the air of social consensus that surrounded the Commissioner’s operations at the outset when almost none of his recommendations had been questioned, now seems to be eroding, as critical remarks are increasingly articulated by the civil sector, the institution’s most powerful former ally.

Historians, particularly those who specialize in recent history, believe they have been disadvantaged by the enshrinement of privacy. Many of them regard the subjects of personal data found in various files and documents as some sort of raw material that is free for the taking, arguing that the individual rights of these subjects should be sacrificed on the altar of research and knowledge of the past. By placing restrictions on the availability of such personal data for research and especially publication, privacy laws indeed limit the access of scholars to documents containing them.

A case in point was the Commissioner’s widely known investigation and “Recommendation on the microfilm recording of documents containing personal data relating to the persecution of Jews during the Nazi period, and on their transfer to the Yad Vashem Archives in Jerusalem”. The Commissioner stated that it was both unlawful and unethical to transfer such documents in the absence of bilateral agreements between the parties. The right to protest against the publicity of their data should also be granted to survivors and their family members, the Commissioner held, with respect to documents already transferred. Following this recommendation, bilateral agreements were signed by the respective governments regulating the relations between Holocaust centers in New York and Jerusalem and archives in Hungary, specifying the terms under which copies of documents were to be transferred, as well as detailing the rights and legal remedies available for the data subjects involved and their relatives.

Among the losers of the changes in recent years we find Hungarian travelers, particularly those traveling to the U.S., who must face data processing practices and treatment often antithetical to European norms. The official Hungarian reactions to the restrictive countermeasures introduced in the U.S. have been a mixed bag. Investigative agencies, the
increasingly profitable security companies, and the political forces that have always frowned on privacy and other informational civil rights. have been only too eager to satisfy American demands, indeed actively seeking ways to collaborate with a great new friend they hope will take the place of a lost powerful ally. All the while, the various institutions safeguarding constitutional values, the DP&FOI Commissioner prominent among them, are defending disclosure of personal data by Hungarian agencies. In their view, such disclosure is based on the “voluntary, unambiguous and well-informed consent” of the data subject concerned.

The broader social reception of these countermeasures is even more ambivalent. Even though the issue has not generated wide public debate, and Hungarian travelers continue to fill out the forms and submit to fingerprinting, they privately voice their suspicion and discontent at such treatment. On the one hand, this phenomenon seems to corroborate the findings of the detailed survey I mentioned earlier, namely that although people distrust power and control over information, they are obedient suppliers of their personal data. On the other hand, it may well be seen as the protracted survival of reflexes of a “secondary public sphere” (the underground or informal public sphere under communist regimes in which developments could be sincerely criticized even if in the official public sphere one had to be a loyal follower of the actual system), triggered perhaps by recollections of life under the totalitarian single-party state.

The ranks of losers also include people targeted by advertising and marketing gimmicks, who realize only too late that by volunteering their data they have unwittingly consented to the unlawful and unethical use of their personal information. Those new (and older) internet surfers, for example, who naively supply their personal details for the sake of participating in an online game, often receive nothing but an unstoppable flood of spams. Paradoxically, the conventional direct marketing industry is one of the winners of a process that has created guarantees for the legitimate pursuit of such business, actually in response to the lobbying efforts of leading DM companies in the mid-nineties. True, privacy guarantees assign limits to the options available for direct marketers – mailing lists can be obtained only from legal sources, the source has to be indicated on every direct mail, “Robinson lists” of individuals who have decided not to receive any direct marketing messages are to be kept etc. But these provisions are lenient enough to allow for profitable operation. Compared to the formerly unregulated situation, the winners include consumers who seek to maintain control of their data and who enforce their right to opt out, guaranteed both by the law and the DP&FOI Commissioner.

V. Information Flows and Constraints: Success and Failure

The single greatest achievement in the struggle for privacy rights was undoubtedly the court decision in the early nineties ruling the standardized and universal personal ID code unconstitutional. Following this around the middle of the decade was adoption of sectoral identification numbers instead, entailing the decentralization of government records and databases.
The critical task for the future is not simply to assign limits to the flow of personal information, but also to give data subjects greater control over their own data. The subject should be free to share or withhold personal data at his or her own discretion.

The Commissioner’s recommendation and positions provide one index of success and failure. The case of the Holocaust documents, for instance, must be regarded as a success: although the Commissioner ultimately refrained from checking the flow of information, he did uphold the right of victims and their relatives to informational self-determination. By contrast, even the Commissioner himself admitted that his intervention against the drive to centralize and re-centralize data had been much less successful. He quoted a number of negative developments such as the centralizing of large personal data processing systems within the Interior Ministry, the broadening of the rights of investigative authorities to access databases, the establishing of the central debtors’ register or the central employment register. All of these developments had legitimate purposes, but all of them significantly exceeded the necessary limitations of people’s informational privacy.

By and large, the Commissioner has been rather successful in investigating egregious violations in individual cases, issuing recommendations and positions of general scope, and promoting the newly acquired informational rights. The overwhelming majority of his recommendations have been followed by the organizations at which they are aimed. On the down side, his activities and the way in which he construed his own role as a specialized ombudsperson with “soft” power have done little to influence the main processes of the democratic transformation in Hungary such as the forming of new systems handling personal information. The Commissioner has often met with frustration in his attempts to deal with violations leading to class-actions violations, the problems of computerized data processing, and the practical implementation of his own registrar functions, i.e. keeping record of data processing operations and data processors.

In addition, the Commissioner’s attempts to tackle the flow of information concerning the operations of agencies that kept the “internal enemies” of the regime under surveillance can ultimately be regarded as a failure. True, he was in an almost impossible situation, struggling to satisfy mutually contradictory calls for historic justice, for the respect of the privacy of victims and third-party individuals, for the vetting and removal of former agents from public office, for the retroactive vindication of the right to informational self-determination of everyone involved, and for what has been called the informational compensation of society as a whole. It is hardly surprising that the severally amended provisions of applicable law and their implementation have failed to unravel the tangle.

To use a metaphor created by the Constitutional Court, the implementation of human rights is a one-way street where you cannot turn back. And yet the space to enforce certain informational rights was narrowed during the period of consolidation that followed the great democratic transformation: The efficiency-minded public administration has increasingly found itself in conflict with demands for privacy protection. Nevertheless, the growth of information processing, as in data mining technologies, should not automatically be interpreted as the failure of the cause of data protection, if the developers, operators and executives of these systems understand that the virtual sum of privacy protection and
business targets is not a constant quantity, one of whose constituents will necessarily grow by the same amount if the other one is reduced. In other words, personal data protection is not necessarily an enemy of business or administrative efficiency.

Fighting for its informational rights and liberties, the civic sector has shown progress in recent years, although it is still quite weak. By and large, civic organizations seldom play a decisive role in questions concerning the flow of personal data, but their influence has been commendable for all its indirectness. Through the Big Brother Awards and other highly visible actions, they can be very successful – if only on a provisional basis – in focusing public attention on privacy values.

**VI. Prospects for the Future**

Hungary, one of the new democracies of Central and Eastern Europe and a new member of the European Union, has now put the shock of collapse of the Soviet bloc behind it. During the initial phase of the new order, the country led the way in instating and enshrining the new rights and liberties. This is a process rife with blind alleys and labyrinths that we cannot fully discern from our vantage today.

It seems that the harmful and excessive politicization of informational rights, and of public affairs in general – as reflected in a wide range of phenomena from the Duna-gate case through extremist anti-privacy political statements quoted earlier to present-day dominance of party politics in the media – is here to stay. None of the successive, democratically elected parliaments and governments of Hungary have managed to change this so far. Therefore, we must look primarily to the political opposition for a stress on the values of informational privacy.

Dispersion of data protection know-how is now under way, with no sign of stopping. This is a welcome process indeed; a single, central organization of expertise and advocacy hardly suffices to bring about the awareness of and concern for these rights among the general public. The current level of civic activism will probably be maintained, as will the dissatisfaction of the sector with the performance of the DP&FOI Commissioner as the chief official proponent of privacy. However, in view of the moderate dynamism of civic movements in general, we should not expect to see a significant growth in the number of these organizations or the actions they undertake.

Hungary is still a far cry from boasting a mature, socially responsible business sector. Most companies and entrepreneurs still regard increased market shares and profits as representing the only valid criteria for business decisions; few executives fully embrace fair treatment of customers as legitimate business concerns in their own right. It seems that entrepreneurs still need to experience spectacular breakthroughs and spectacular defeats before they can make room in their value systems for the service of public good and the respect for the rights of customers as individuals and data subjects. (This is what happened for example in the high-tech sector in the US, when, after the 2001 collapse of the market, some of the firms redefined themselves as socially responsible for-profit companies or social
enterprises.) Concurrently, we can discern the outlines of another, unfavorable tendency as we witness the controllers of information in the public sector join efforts with their private-sector counterparts vis-à-vis the citizen, whose position in its citizen-type transactions begins to look increasingly like that of the customer as a result. Examples of this tendency can be found in the outsourcing of public functions, including the processing of personal data concerned, or in the cooperation of state registration systems and private insurance companies.

In 2004, Hungary’s data protection law made it mandatory for a variety of organizations processing personal data to appoint their own internal privacy officers. Courses have been held to prepare them for this task. Some of these officers continue to fulfill a largely symbolic function, but the strongest among them are successful in raising the level of privacy awareness and know-how in their organizations. This trend is expected to pick up speed in the near future, aided in part by the limited but highly professional practice of voluntary data protection audits. These audits are conducted by specialists at the request of large banks, insurance companies, direct marketing firms and other data controllers in the public and private sector, including the Government’s Portal.

In the business sector, privacy performance is strongest among companies with a mother company headquartered in a foreign country with strong privacy laws. For example, German-based businesses tend to improve the corporate culture of privacy within their Hungarian subsidiaries. German ownership in big telecommunication companies like Magyar Telecom has a similar effect. Specialized training also makes an important contribution. Although information technologists usually side with the data processors, they can be quite privacy conscious if exposed to the values of privacy in the course of their studies. Any curricular item they have to master in this field, including Privacy Enhancing Technologies (such as anonymous browsers to be used by internet users) and IT solutions to be adopted by data controllers (such as segmented access control to customers’ personal data), will indirectly shape their mentality, conceptual framework, and work as developers.

The ways in which personal data are handled in the public sector will undergo significant changes with the realization of the visions of e-government, the rising number of public services available through the internet, and the increasing use of the universal client gate. Such a virtual gate where the citizen enters the sphere of electronic governmental services, without proper rules of handling personal data, can lead to a situation in which government offices interchange and use citizens’ data without citizens’ awareness and control over the fate of their data. Happily, the agencies currently in charge of developing e-government services have displayed a healthy attitude to privacy concerns. Admittedly, though, the right attitude in itself will not guarantee the acceptable implementation of these systems.

In the international arena, we can expect the U.S., NATO, Europol and other intergovernmental organizations to step up pressure on Hungary and other new European democracies to appropriate their citizens’ data and to place restrictions on their citizens’ informational rights. The main areas are mandatory data sharing with foreign law enforcement agencies, data retention as well as monitoring of private communication such as mobile calls or e-mails, and broadening of the sphere of classified information. We have
already seen the signs of policy laundering. This is the process in which measures that
would be disqualified by the constitution and legal system of a democracy are first exported
to an international organization, then subsequently re-introduced for domestic use. Such an
attempt could be experienced in early 2005 at the so-called Salzburg Forum, the gathering
for the cooperation of six Central European countries in the area of home affairs. At a Forum
session Hungary submitted a proposal in order to remove obstacles to the use by the police
the EURODAC database, which contains the personal data and fingerprints of refugees and
illegal migrants. Such a proposal would be surely disqualified under Hungarian law but there
is much more chance to introduce it through the EU. This tendency is going to continue in
the future.

There are also home-brewed attempts in Hungary at restoring the old, centralized personal
information regime. To give one notable example, the Hungarian Academy of Science has
set up an ad hoc committee which actively promotes such a restoration. Its members include
representatives of government bodies with vested interests in concentrating data processing
capabilities (among others, to stimulate more extensive use of their e-Government services),
as well as private companies steered by information technologists who used to work for the
Ministry of Interior and continue to accept contracts from the government, and finally a few
scientists whose field of specialization and ideology have to do with the “wiring” of the
planet. The barely disguised ambition of this committee is to bring back the old universal
personal ID code, and ultimately to render the data of every citizen free prey to all
organizations, public or private. It seems unlikely that these efforts will succeed. But it
would be foolish to underestimate the forces the committee has managed to mobilize, or the
powerful political and business interests behind them.

In Hungary – as in other countries that overhauled their political systems in the first wave of
democratization in the region – the euphoric elation and momentum of metamorphosis is
now spent. This marks the end of boom in the respect for individual rights, including
informational ones. László Majtényi, the country’s first DP&FOI Commissioner, once bitterly
observed that “The constitutional revolution in Hungary has failed.” While I would hesitate to
go this far myself, I concede that a new, much more technocratic generation has grown up
for whom career, profit, business, and political power all take precedence over respect for
individual rights, most notably those concerning the uses of information.

For the years ahead, I predict that new business solutions and e-government strategies
based on the latest information and communication technologies will continue to redefine the
nature and the scope of the ongoing debate – or should I call it struggle – over the handling
of personal data. This is precisely why it would be vital for this new generation to
permanently embrace the values of privacy. Only then can we ensure that these values will
be reflected back upon us by the data processing systems of the future and the ways in
which we will elect to use them.
References

Act No. V of 1878 (Csemegi Codex), *A magyar büntetőtörvénykönyv a büntettekről és vétségekről* [Hungarian Penal Code of criminal acts and offences]


Szladits, K. (ed.) 1941, *A magyar magánjog* [Hungarian Civil Law], Grill K., Budapest