Chapter 4
From a Model Pupil to a Problematic Grown-Up: Enforcing Privacy and Data Protection in Hungary

Ivan Szekely

4.1 Introduction

When the new democracies of Central and Eastern Europe had to implement the rights of the western world, they had to choose the particular mechanisms of enforcement. Among these new rights and freedoms, the information rights, which included the right to privacy and data protection, featured prominently in the priority list of the democratic transition. In the 1990s, Hungary proved to be a model pupil in the creation of the system of information rights and, through the establishment of an ombudsman-type institution to safeguard data protection, it also led the way in developing the enforcement mechanisms. For more than 15 years, the data protection ombudsman headed one of the most successful new democratic institutions in Hungary, while the country itself served as an example to the other new democracies of the region. However, the government that took power in 2010 decided to abolish the institution in 2012, dismissing the data protection ombudsman before the end of his mandate and setting up a new government authority for enforcing of the data protection laws. This amounted to a paradigm change in the enforcement mechanisms, and the method chosen to carry this out provoked strong criticism from several international organisations. While it is still too early to assess the impact of the paradigm change and the performance of the new authority, the story of enforcing privacy and data protection in Hungary can definitely offer important lessons for other new democracies. This chapter describes and analyses how privacy has been enforced (or not) in Hungary since its transition to a democracy in the early 1990s.

History tells us that in the case of those countries that experienced an abrupt change in their political and social system as they moved from a closed, authoritarian
regime or an outright dictatorship to a more open, democratic system based on
western liberal values and the rule of the law, the codification of the new rights and
freedoms, together with the formation and functioning of their enforcement
methods and institutional system, and the public’s respect for them, tend to show a
characteristic pattern in their evolution.

In the period immediately after the democratic transition, these rights and free-
doms are usually regarded as being of the highest importance; some of them, for
example, the right of assembly or the freedom of information, often become the
symbols of, and the practical tools for, staging a break with the old political system.
The sufficiently active and professionally well prepared countries, which are usually
the most successful in codifying the new rights at this early stage – and not
merely in an ad hoc manner but proceeding systematically in transforming the entire
legal system on the basis of the western standards of constitutionality – have reason
to feel historically lucky, in the sense that in subsequent periods of far less favour-
able circumstances, they are able to preserve the basic institutions of democracy and
the rule of the law. The first period of euphoria is almost invariably followed by a
period when people discover that the new rights and the new legal institutions will
not be able to solve the country’s social and, more importantly, economic problems,
while the more liberal environment will allow the influential players of the old
regime to retain their former influence and control. The formation of the new eco-
nomic and political power structures begins, in which the realisation of the indi-
vidual freedoms might seem to act as a limiting factor; and within a few years, a new
generation emerges, whose members are no longer interested in the past and only
care for the present, and whose main ambitions concern material goods, individual
advancement and the development of new power structures in the interests of which
they are sometimes willing to transgress legal and ethical norms. ¹ All these together
lead to the erosion of the respect for, and importance of, the constitutional values
and the new rights and freedoms, and the process is usually accompanied by a
decline in the acceptance of both the enforcement methods and associated
institutions.

This chapter does not discuss the democratisation processes of the countries of
the cultural East, where the substantive acceptance of both the influence of the west-
ern values and the rights and freedoms understood in the western sense pose funda-
mental theoretical and practical problems anyway. Instead, it focuses on the “new
democracy” of Hungary, a representative of the region that for a prolonged period
had belonged to the Soviet bloc and followed a Soviet-type political and social
model. The above-referenced evolution pattern reveals distinct, country-specific
features within the region; the time and the scale of the changes vary from country
to country. Nevertheless, there are historical experiences of general validity, which
might even serve as instructive lessons for some new democracies to emerge in the
future.

¹For an analysis of freedom of information in Central and Eastern Europe, see Szekely, Ivan,
“Central and Eastern Europe: Starting from Scratch”, in Ann Florini (ed.), The Right to Know:
The right to privacy is one of the fundamental rights, which made their appearance in the legal framework of the new democracies either during the turbulent years of democratic transition or in the period immediately following. The countries concerned (the former communist countries of Central and Eastern Europe, the so-called Soviet Bloc) did not have the necessary time to fully develop these rights and to incorporate them in their legal and institutional practices in the course of a long, organic development, so as to consolidate their social embeddedness or interiorisation, i.e., to become an accepted part of the social fabric. As a result, the rights to privacy and data protection had to be imported from the practices of the more fully developed democracies, along with many other legal principles and norms. In addition, suitable points had to be found for linking them to the existing legal and institutional traditions, and even to the current legislative framework, especially in those countries where the democratic transition had been completed without bloodshed, through the peaceful transfer of power. In the context of Hungary, the implementation of these new laws is of great interest, since, on the one hand, it provides an excellent example of the establishment of the new legal order and the consolidation of the institutional and enforcement system and related practices, while on the other hand, it faithfully illustrates the vulnerability of a system considered to be firmly established and well functioning, along with its sensitivity to changes in the political environment, and thus – not at all independently of the international trends in the enforcement of privacy law – it reveals radical changes in the model.

The following pages briefly outline the emergence of privacy and data protection legislation in Hungary after the democratic transition in the 1990s, mainly concentrating on the formation of the enforcement mechanisms and the associated institutions. The chapter then describes the political and social context and the functioning of the new institutions, and discusses the fundamental changes that have taken place in the political and legal system since the early 2010s. This chapter has a special focus on the enforcement model of privacy and data protection laws. Next, it analyses those aspects of the legal and enforcement guarantees in the privacy and data protection laws that are specific to Hungary, revealing the origins of these developments and pointing out the causes and consequences of recent changes in them, while also mentioning the main differences between the two models. After that, the chapter demonstrates the differences between the two models through a few typical examples of the mandates and the roles of the former data protection ombudsman and the present data protection authority, respectively.

Since the history of enforcing privacy and data protection legislation is far from its end in Hungary, we conclude our analysis by posing a few open questions, followed by a few general recommendations for the new democracies in area of privacy and data protection taking into account historical experiences.
4.2 A brief history and context

Before the Second World War, Hungary was still not in the position to generate demand for western-type information rights and to organically build it into the country’s legal system; during the decades after the war, it was no longer in the position to do so. That could only take place in the hectic period around the 1989 democratic transition, almost as if to make up for the lost decades. The scant legal precedent mostly came via those comrades who had encountered the ideas and expectations of information rights, including privacy and data protection, at conferences abroad, manifested in the introduction of some new provisions in the Communist legal system, partly as a result of a cautious adoption of western expectations, and partly simply due to some misunderstandings.\(^2\) The most important and most substantive precedent was the creation of a multidisciplinary experts’ team,\(^3\) which worked under the auspices of the Central Statistical Bureau (KSH): it collected the international examples of data protection and freedom of information; it developed the legal regime for the new information law still before the democratic transition, including a draft proposal for the combined data protection and freedom of information law.

There was a negotiated transfer of political power, a “velvet revolution” of some sort. The platform of the negotiations was called the Opposition Roundtable (EKA), which brought together the leaders, spokespersons and experts of the old and the new regime. Even the participants of EKA could sense that they were in fact making decisions about the transformation of the political and legal system without consulting the people, so they tried to establish legal institutions, which would belatedly allow the citizens to have a direct say in the running of public affairs. As Laszlo Solyom, participant of EKA (who later became President of the newly established Constitutional Court, and then President of the Republic), stated at a conference held recently\(^4\), the EKA made three “gestures” to the people: the establishment of the institution of ombudsman (“the people’s advocate”),\(^5\) the introduction of the *actio popularis* (the option to turn to the Constitutional Court directly) and the creation of the conditions for holding referendums.\(^6\)

A milestone on the road to the creation of the data protection law was the 1991 decision of the Constitutional Court, in which it declared the use of the universal personal ID number to be unconstitutional, expounded the principles of information self-determination patterned on the German model, and ordered the Parliament to

---

\(^2\)For example, data protection was often confused with data security.

\(^3\)Laszlo Solyom was among the members of this group, as were Laszlo Majtenyi, the first data protection ombudsman, and the author of this chapter.

\(^4\)Conference on the institution of constitutional complaint, organised by the Eotvos Karoly Policy Institute on 21 February 2014, in the OSA (Vera and Donald Blinken Open Society Archives at Central European University), Budapest.

\(^5\)The data protection ombudsman became one of them.

create a data protection law. Parliament passed the law in 1992, without a single opposing vote. This combined data protection and freedom of information bill prescribed the establishment of an independent supervisory body, the office of a parliamentary commissioner with ombudsman-like powers. However, this only took place in the summer of 1995, together with the election of the other two parliamentary ombudsmen.

The data protection ombudsman (Parliamentary Commissioner for Data Protection and Freedom of Information), who was responsible for supervising the enforcement of both information rights, functioned between 1995 and 2011 and his office was one of the most successful institutions of the new democracy, the practices of which were taken as a model by several similar institutions in the West. As for Hungary, it became something of a model country among the new democracies in the area of the introduction of information rights. Nevertheless, the political leadership that took power in 2010 abolished the institution and dismissed the data protection ombudsman before the end of his mandate, creating instead a government authority – which was not a legal successor – effective from January 2012.

4.3 Characteristic features: the causes and the consequences

Constitutional values become part of the legal framework only when their codification is followed by the establishment of enforcement mechanisms. The laws come to life and become socially embedded only after these values have been accepted both by the institutions and administrators of the public sphere and the civilian population, when these laws are widely understood and when the legal institutions are broadly used.

The question about the extent to which these constitutional values – including privacy – became interiorised both by the public and the political elite during the turbulent years of democratic transition and the extent to which they had been latently present in the period before the transition is worth asking. During the decades before the democratic transition, such questions were primarily addressed by a Hungarian institute unique in the entire Soviet bloc, the Mass Communication Research Center (TK). Throughout its existence between 1969 and 1991, the TK – in its final years, renamed as Hungarian Institute for Public Opinion Research (MKI) – carried out investigations in the areas of public opinion and mass communication, operating on a generous budget, maintaining a very high professional standard, and using the most up-to-date methodologies developed in the western world. However, the first democratically elected government after the transition abolished the institute on the grounds of its former co-operation with the old regime; the research continued in the 1990s within a different organisational framework, based on a less coherent methodological foundation.7 Happily, young researchers can

---

7The research centres and private polling firms, which now mostly work as the Hungarian subsidiaries of international polling companies, originally were formed from the institute’s professional
benefit from empirical studies that had already been conducted prior to the democratic transition\textsuperscript{8} and that continued into the 1990s.\textsuperscript{9}

From the viewpoint of our topic, a survey conducted in 1988–1989\textsuperscript{10} is perhaps the most important: this was the first effort in the region to conduct a comprehensive survey about public opinion concerning privacy, data sensitivity and trust in data-handling organisations. An analysis of the findings showed that people had substantive views about these apparently rather abstract issues, and although these opinions were somewhat uninformed, with the help of multivariable methods, the main patterns of views can be demonstrated. According to these, crucial factors were sensitivity to privacy issues, receptiveness to trust and order, and pro and anti-computer attitudes.\textsuperscript{11} Although the respondents in general revealed a considerable degree of mistrust towards the proprietors and representatives of information power, the overwhelming majority of them were compliant data subjects: resistance to data requests was rarely recorded.\textsuperscript{12}

The interiorisation of values is important, since the task of raising awareness for the rights and values of privacy and data protection, or more generally the job of working out the system of information rights and developing the enforcement mechanisms and the associated institutions, mostly fell on an elite team, which embarked on these tasks well before the period of the democratic transition. In some sense, therefore, the establishment of the new system of information rights can be regarded as an “elitist” initiative, which in numerous situations has become a useful reference point for the political system in connection with the western democracies or the international organisations, yet for the entirety of the public administration or

\begin{footnotesize}

\textsuperscript{8} The important question one needs to ask is how far can one trust the data of public opinion polls recorded under a dictatorial regime, and whether what the respondents say can be accepted as their own opinions. Participants of the conference “TK 3.0: Did People Lie in Kadar’s Hungary?”, which was held in April 2013 at the OSA concurred in the view – in harmony with earlier professional opinions – that the surveys conducted by TK had yielded authentic information about public opinion; it came with the price that certain parts of these research results could never be published before the democratic transition.

\textsuperscript{9} Much can be learned from the comparison of two surveys, which used similar methodology to find out about what was better in Hungary than in the West in public opinion. In 1981, a considerable majority of the respondents thought better of the Hungarian situation in all of the areas (including the general moral condition of society, the well-balanced lives of families, and the freedom of opinion), while by 1987, the scenario had radically turned around. A retrospective analysis of these surveys can show not only the changes in values, but also the radical weakening of the regime’s legitimacy in these years. See Vasarhelyi, Maria, “Lattuk-e, hogy jon?” [Did we see it coming?] \textit{Jel-Kep}, No. 3–4, 2010, pp. 91–97.

\textsuperscript{10} The research documentation and the data files are now held in the OSA.


\textsuperscript{12} The complete English-language study is available at \url{http://www.sscqueens.org/sites/default/files/Information_Privacy_in_Hungary.pdf}

\end{footnotesize}
the broad segments of the population, it is becoming a familiar and accepted idea only slowly and gradually.

In view of the fact that in the period before the democratic transition, people had only a limited ability to realise the right to privacy, or even to learn about its content, readers may be surprised by the first data protection ombudsman’s assessment of the situation, who wrote the following in his first report:

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.\(^\text{13}\)

Indeed, such a positive assessment was supported by the surveys conducted in the 1990s to test knowledge and legitimacy\(^\text{14}\); subsequently, the knowledge index of the office of the data protection ombudsman increased,\(^\text{15}\) while the trust index declined\(^\text{16}\) (this can be seen as another example of the evolution patterns mentioned in the Introduction). Parallel with this, new voices arose in the changing political landscape, which questioned the extent of data protection laws and the need for the enforcement mechanism, while a radical right-wing politician went as far as saying that the office of the data protection ombudsman should be abolished, because the concept of data protection is alien to the Hungarian national spirit.\(^\text{17}\)

From a legal perspective, the consolidation of privacy and data protection legislation proceeded in instalments, in a typical top-down fashion: first, the basic provisions were inserted in the Constitution; next, the newly established Constitutional Court issued rulings to expound its content, after which the Data Protection Act was formulated and work on sector-specific laws began, and finally the independent supervisory body was established.\(^\text{18}\) The model had three distinct features: (1) the rights


\(^\text{14}\) According to a 1998 survey by Szonda Ipsos, 43 % of the population knew about the data protection ombudsman, and the ombudsman’s office in general ranked fourth in the list of most trusted institutions (after the President of the Republic, the Constitutional Court and the respondent’s favourite political party).

\(^\text{15}\) According to the results of the survey repeated 10 years later, in 2008, 46 % of the respondents had heard about the institution of data protection ombudsman, which earned Hungary second place among the countries of the European Union (Flash Eurobarometer 225, [http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf](http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf)).

\(^\text{16}\) According to a 2008 survey by Szonda Ipsos, the trust index of the institution of ombudsman dropped from 63 to 52 % in 10 years (it must be pointed out, however, that the trust for institutions in general was also declining at the time).

\(^\text{17}\) Istvan Csurka, chairman of the Hungarian Justice and Life Party, Spring 2001. See [http://www.origo.hu/iththon/20010426antidemokratikus.html](http://www.origo.hu/iththon/20010426antidemokratikus.html) [in Hungarian]. The political attacks led to the obstruction of the first data protection ombudsman’s re-election; the post was eventually filled after a 6-month delay.

\(^\text{18}\) Although the possibility of enforcement through court action already existed before the introduction of the independent supervisory body, this hardly ever happened in practice. (This partly proved that there was a real need for the creation of a specialised supervisory and enforcement institution.)
to privacy and data protection which were elevated to the status of fundamental
rights enshrined in the Constitution; (2) informational self-determination conceived
along the lines of the German model (thus raising the standard above the minimum
level required by the Council of Europe and the European Union); and (3) an
ombudsman-type supervisory body. A further characteristic of the legislative model
was the structural division of general law versus sectoral laws: the data protection
law – covering both the public sector and the private sector – laid down the funda-
mental rules for handling personal data in a codex-like manner, while the sectoral
laws and regulations mainly contained the detailed provisions and, most notably, the
exceptions; in matters not covered by the sectoral rules, the provisions of the data
protection law automatically applied.19

With the exception of the type and mandate of the independent supervisory body,
all the rest of these characteristic features have survived down to the present day
(even though the codex-like character of the data protection law has partially eroded
due to the numerous exceptions and subsequently introduced legislative changes).

So how can the characteristic features of the Hungarian model be explained? On
top of the historical, legal and administrative traditions (traditions that reached
Hungary with a delay and manifested themselves only in a twisted way in the
decades prior to the democratic transition), one of the causes was provided by the
specific experiences of the dictatorial regime and by the effort of the new system’s
constitutional fathers to raise the level of the legal guarantees of the new democratic
establishment as high as possible, as a precaution against a possible reversal of the
democratic process, should a future power try to take back the newly gained and
codified rights.20 This, too, contributed to the fact that the level of data protection in
Hungary – similarly to other, post-dictatorial countries – was set at a level that in
many respects was distinctly higher than the minimum standard for European
democracies. Other factors that contributed to the development of the model were
the legal systems of western, most notably European, democracies, the legal and
institutional models they had developed, and the practical knowledge they had
gained in the realisation of privacy and data protection.21

However, the role, erudition and approach of certain prominent persons cannot
be overlooked – this was especially important in regions where the reforms and the
changes had an “elitist” character, advanced by a vanguard of professionals, rather
than some plebeian mass movements. The prime mover in the adoption of the
German model – including the concept of informational self-determination – was
the law professor Laszlo Solyom, who in the second half of the 1980s studied on a

19 For more on this, see Szekely, Ivan, and Mate Daniel Szabo, “Privacy and data protection at the
workplace in Hungary”, in Sjaak Nouwt, Berend R. de Vries and Corien Prins (eds.), Reasonable
Expectations of Privacy? Eleven Country Reports on Camera Surveillance and Workplace Privacy,
20 The political elite of the democratic transition proved to be less circumspect in making the whole
of the constitutional system impervious to these kinds of changes, as vividly demonstrated by the
recent political changes related to constitutionality.
21 In the collection and analysis of these, the earlier mentioned interdisciplinary team working
under the aegis of the KSH played a prominent role.
research grant at the Johann Wolfgang Goethe University in Frankfurt\textsuperscript{22} under the supervision of Spiros Simitis, a prominent scholar of German and EU data protection legislation, whose name was associated with the drafting of the first data protection law\textsuperscript{23} and who filled the office of data protection ombudsman in the province of Hessen for 15 years. In a broader sense, Solyom also prodded the Hungarian Constitutional Court into adopting certain practices, and occasionally even the concrete reasoning, of the Constitutional Court of Germany. Solyom was later elected as the first, and probably the most influential, president of the Hungarian Constitutional Court; he eventually became President of Hungary in the period between 2005 and 2010.

The other person who had a major influence on developments in the area of data protection in Hungary was Laszlo Majtenyi. He learned about the Scandinavian model of the ombudsman system while studying on a scholarship in Norway. Through the articles he published in professional and public journals, he presented this model to the Hungarian experts in charge of developing the new legal and administrative system, personally making tremendous efforts to integrate it into the Hungarian legal and administrative system. As Hungary’s first data protection ombudsman, Majtenyi was responsible for creating the legal environment for the ombudsman system, developing the rules of operation and defining the main priorities of its activities.\textsuperscript{24} Of course, the influence of one person would not have been enough to bring about the establishment of the ombudsman system in Hungary: the process was greatly aided by the view – widely held in the countries of Central and Eastern Europe – that the introduction of a previously unknown institution, the office of the ombudsman, could work as some kind of a panacea in solving the country’s problems concerning public administration, civil rights protection and the self-correction mechanism of the new democratic system in general.

\subsection*{4.4 Enforcement models and alternatives}

In the period following the establishment of the data protection ombudsman, three types – or models – for enforcing privacy and data protection laws appeared in the Hungarian legal system. The most robust among them was the functioning of the data protection ombudsman, which was based on a powerful mandate to investigate

\textsuperscript{22} Later on, when he was already President of the Republic, the university awarded Laszlo Solyom an honorary doctorate (“Sterne unserer Jugend – Ehrendoktorwürde des Fachbereichs Rechtswissenschaft für den Ungarischen Staatspräsidenten Prof. László Sólyom”, \textit{UniReport} 7, 15 November 2006, p. 2. \url{http://www2.uni-frankfurt.de/44481170/unireport_07-2006.pdf}).

\textsuperscript{23} The federal state of Hessen, 1970.

\textsuperscript{24} Although the official title of the – by now abolished – position was Parliamentary Commissioner, the public usually referred to him as data protection ombudsman, just as they did to the other two varieties of parliamentary commissioners.
and a weak mandate to enforce: in other words, it had the characteristic features associated with the activities of the ombudsman, exerting an influence through recommendations and voluntary compliance, as well as through the power of publicity. Its investigative powers were among the strongest within the structure of the State, surpassing even the powers of the other parliamentary ombudsmen: it could request information from any of the data controlling organisations within both the state and the private sector in all matters related to personal data (or data of public interest); it could inspect or copy all documents and enter all offices where data were processed, and in these activities, it could not be hindered by state secrets, trade secrets or other confidential information.\footnote{Act LXIII of 1992, Section 26 (1).} As the annual reports of the data protection ombudsman have shown, its weak powers to enforce were accompanied by the high rate of voluntary compliance, which proves the success of the ombudsman model.

However, even the data protection ombudsman’s powers mixed investigative authority with enforcement authority, although the few enforcement-type authorities assigned to it from the beginning were associated with its other main task, the supervision of access to public information – and classified state secrets, as a limiting factor. If the ombudsman thought that the classification of some information, or its time limit, was unjustified, he could instruct the data controller to modify or abolish it.\footnote{Section 26 (4) [renumbered as (5) after a subsequent modification].} The data controller concerned then had the right to appeal to the court against such an instruction, as an example of the checks and balances between organisations of the State.

After the amendment of the law in 2003 – initiated in order to counter the slight decline in the number of voluntary compliances – the data protection ombudsman was empowered to issue binding decisions as part of his competences related to the protection of personal data: once the data controller refused to accept the ombudsman’s recommendation, the latter gained the authority to issue a binding decision to prohibit or to suspend the further processing of data, to delete or destroy the personal data processed illegally, or to suspend the forwarding of the data to a foreign country. But in practice, the ombudsman resorted to this power only in cases when all his other options had been exhausted, as he continued to perceive his role as an ombudsman. On the other hand, the duties of data controllers became more robust and better defined: data controllers had 30 days to respond to communications (recommendations or decisions) from the ombudsman, the same time period they had to appeal against decisions in court. However, the proceedings hardly ever reached that stage, and if they did, they mostly took the form of a trial case, in which the data controllers usually withdrew their appeals before the court’s issuing its decision. In general, it is fair to say that even in this period, the investigations of the data protection ombudsman – when they confirmed the unlawful processing of personal data – mostly ended with the data controller’s compliance, and in those few instances when he felt the need to issue a binding decision, these were mostly carried into effect. These characteristic features of the data protection ombudsman’s mode of operation survived right until the abolition of the institution.
Although the data controllers’ willingness to accept the ombudsman’s recommendations and decisions could be observed as a rule throughout the period, some of the data controllers resorted from the start to the tactic of deftly evading compliance with the measures required by the ombudsman. One method of such evasions was formal compliance, when the data controller accepted the ombudsman’s recommendations at the level of declarations, but continued with the substandard or unlawful data processing in practice.\textsuperscript{27} A similar practice could be observed in connection with the various government offices, which tried to ward off the ombudsman’s critical or inconvenient remarks in his legally required evaluation of any draft legislation by failing to send the ombudsman’s office a copy, or by sending it only at the last minute. This, of course, could also have resulted from simple carelessness (although that, too, would say a lot about the prestige of the data protection ombudsman’s office in the government’s eyes), but the assumption of intentionality would not be too far-fetched. This practice took several forms (the data protection ombudsmen all made a note of these in their annual reports), one of which was sending drafts running to hundreds of pages without marking the places where the ombudsman’s comments were required, in the hope that his assistants may have missed the relevant passages; or sending large volumes of texts on a Friday afternoon, with a return date by Monday morning. The element most likely to draw criticism in connection with the involvement of the ombudsman in the legal review process was the decision to put it in the general review round, where his opinion counted as only one among the views of many other organisations, occasionally as many as 50, and so in the end, it hardly received the necessary attention. A more appropriate solution – one that was more in line with the legal status of the ombudsman – would have been if the government, in the course of the preparatory phase of the legal drafting – had first held a preliminary consultation among the governmental bodies, before sending the agreed draft proposal to the data protection ombudsman, who then could have added his own remarks and recommendations to it, which – in the case of parliamentary legislation – could have been presented to Parliament alongside the government’s proposal.

The other method of formal compliance was based on a ruse analogous to the practice of journalists under the communist regime of earlier times, who added a “red tail”\textsuperscript{28} to their articles. The “red tail” treatment in the form of a “data protection tail” was applied every time when a blatantly unlawful method of data processing (to which the ombudsman was likely to object) was announced and the data controllers wanted to promote it. In introducing a new plan, which concerned the processing of personal data, or sometimes even in launching an entire system developed

\textsuperscript{27}This mostly happened in the case of service providers with a large number of domestic clients, according to the experience of the author who had, earlier on, worked as an expert and advisor – naturally, bound by very strict secrecy obligations.

\textsuperscript{28}In the period of the thawing of the communist ideology during the Kadar regime, journalists were able to praise the achievements of the capitalist system almost in any areas, providing they ended the article with a turn of phrase something like “the future belongs to communism” or “the world’s leading power is the Soviet Union” – this was to what the term “red tail” referred.
without the involvement of the data protection ombudsman, they invariably ended their presentation with the turn of phrase “in full compliance with the relevant sections of the data protection laws” — even when the system in question had obviously been created and operated in violation of the provisions of the data protection law. Finally, in addition to the tactics of evasion and deceit, open resistance to the data protection laws and the data protection ombudsman had also raised its head by around 2005; it was led by the experts of the efficiency-conscious bureaucracy (former supporters of data protection legislation), allying themselves with the representatives of the information industry, who had earlier looked upon the centralisation of registries and personal identification systems, and their legitimate use for any purpose, as the “modern” ideal. These efforts were taken on by the Institute for Computer Science and Control, Hungarian Academy of Sciences (SZTAKI), 29 which took care to also invite a former data protection ombudsman as well as some independent experts in data protection 30 — making sure, of course, that any dissenting opinions by the latter remain in the minority, and occasionally seeing to it that those views were watered down in the minutes taken at the discussions. 31

All in all, it is fair to say that the office of the data protection ombudsman has successfully foiled the attempts to soften the information rights regime. However, in some areas, the data protection ombudsman was only able to accomplish moderate results, and these were all related to issues of enforcement. One of these issues concerned the running of the central data protection register, which contained the most important information related to data processing and data controllers, and which is accessible to anyone. The system providing online access to the register itself took long years to complete and the design of the user-friendly interface left much to be desired, but it was mainly in the area of improving the slack discipline in reporting in the various sectors of data controllers that the ombudsman and his office proved less successful or at least inactive. The data protection law required data controllers to file an annual report about the number of personal data requests they turned down each year, and the specific grounds they cited (the ombudsman annually issued a call in the official bulletin to that effect). And while they were not obliged to provide information about the successful requests, the ombudsman — on a voluntary basis — encouraged the data controllers to do so. Neither the range, nor the information

29 The broader framework of the initiative was the establishment of an ad hoc committee by the President of the Academy of Sciences in 2005, which dealt with “the conceptual issues of information society and the most burning problems of society management (sic) at the moment”. The chairman of the committee was the academy member Tibor Vamos, the president of SZTAKI.
30 When the committee completed its report in May 2006, Laszlo Solyom, whose “persuasion” the committee regarded as crucial, fulfilled the office of the President of the Republic. The incumbent data protection ombudsman was not invited to participate in the committee’s work.
31 This lobby eventually was successful, in the space for manoeuvring created after Laszlo Solyom’s term as President of the Republic had ended, the institution of the data protection ombudsman had been abolished, the constitution had been rescinded and the new law replacing the data protection law had been passed, clearing the way to revoking the ban on the standardised and universal personal identification number, which had been one of the symbols of opposition to the dictatorial regime in the area of information law.
content of these reports can be described as satisfactory; for this reason, it is impossible to draw conclusions from this data.\footnote{The ombudsman regularly gave a detailed account of this activity in his annual reports.}

Several data protection ombudsmen questioned the usefulness and functionality of the data protection register and the filed information on turned-down requests, but that was not what mattered most: it was the use of the single search and retrieval system for data of public interest that explained the ombudsmen’s moderately successful supervisory authority. Rather than his mandate to protect personal data, the ombudsman’s authorisation to act in matters regarding the accessibility of public information was affected by the system: the law of 2005 on the freedom of electronic information\footnote{Act XC of 2005 – its provisions were later incorporated into Act CXII of 2011, which replaced the data protection law.} made it mandatory for government organisations, local government agencies and other organisations performing public functions to display certain information relating to their operation and financial record on Internet websites, and to register the metadata of this information in a standardised search and retrieval system for data of public interest. Interested citizens can then access current and relevant public information through this standardised system. But a precondition is for the organisations obligated to provide information to register in the standardised system and to regularly update the data and documents for the website. Compliance with the requirement to register and to update – regardless of the technical adequacy of the system – was very poor; moreover, the ombudsmen did not make the necessary effort to encourage co-operation on the one hand, and to sanction failure to comply with a legal obligation on the other.

Finally, we must point out that during the 17 years that passed between the establishment and the abolition of the data protection ombudsman’s office, the different personalities of the three data protection ombudsmen greatly determined the character of the institution’s activities. Experience has shown that all ombudsman-type institutions are, by their nature, highly susceptible to the leaders’ personality, and since they have considerable freedom in shaping the operative rules of their institutions themselves, the institutions end up reflecting the approaches and priorities of their leader. To sum it up briefly, the first data protection ombudsman, Laszlo Majtenyi, emphasised the ombudsman-like character of the institution; the second ombudsman, Attila Peterfalvi, focused more on the efficient functioning of the office, while András Jori, the third and last ombudsman (who was dismissed from the job before his term expired), paid special attention to the data protection aspects of new technologies.\footnote{The similarities and differences between the respective approaches of the three data protection ombudsmen were revealed to the public at a roundtable discussion held during the last international professional conference before the abolition of the institution (“Data Protection Commissioner: 1995–2011”, 28 September 2011).}

The second type of enforcement, enforcement through public proceedings, appeared in specific sectors of data processing, such as telecommunications or banking, where the supervisory body overseeing the legal provisions of the activities...
in the given area was also responsible for monitoring compliance with, and sanctioning violations of, the relevant sector-specific laws of data protection. From time to time, this additional possibility and the accompanying public authority character turned out to be useful for the data protection ombudsman, too: when the data controllers in these sectors failed to comply with the data protection ombudsman’s recommendation or decision – and a court proceeding was not possible – the ombudsman could turn to the body supervising the given area and ask the supervisors either to penalise the data controller or to enforce the acceptance of the recommendation or decision through other available disciplinary measures. Such actions could be taken in the financial and telecommunication sector, among others, where the supervisory bodies have already imposed high penalties for the illegal and unnecessary practice of photocopying personal identification documents. Such cooperation in some areas increased the efficiency of enforcement and, as a result, the data controllers started to take the data protection ombudsman’s recommendations and decisions more seriously.

The third, traditional type of enforcement was legal action in a court of law. This course has always been open to both data subjects and data controllers, yet it was relatively rarely taken, in comparison to the number of proceedings taken by the data protection ombudsman. In contrast to the thousands of applications sent annually to the ombudsman, the number of court actions in data protection cases was limited. Our study of these court cases was greatly facilitated by the Compendium of Court Decisions, an institution created by the Electronic Freedom of Information Act of 2005, with online access open to anyone. This database reveals that, on the one hand, in the majority of cases with some bearing on this subject, the processing of personal data does not form an essential point of the case and, on the other hand, both the data controllers and the data subjects regard the personal data related to customer relationship and customer service as data forming part of the business procedure, rather than as personal data in the sense of data protection law.36

Whether it was about data subjects worrying about the possible violation of their data protection rights or about data controllers considering the data subjects’ legal actions as unjustified, what the people in question needed to consider was the relative advantages and disadvantages of the different procedures. Adjudication by the data protection ombudsman was cost-free – regardless of the outcome – while a court procedure involved certain costs (court fees, lawyers’ fees and stamp duties). Even if you would not exactly describe it as fast, the ombudsman’s procedure was quicker than court action (despite the fact that the data protection law required the courts to hear such cases in priority proceedings). On top of that, the ombudsman’s

35 In this way, the data controllers in fact had withdrawn behind the walls of passive resistance; as the ombudsman had no means to enforce the decision an impasse followed in the execution of the data protection law.

36 This latter phenomenon was confirmed by the empirical research conducted in an ongoing EU FP7 research project, IRISS (http://www.irissproject.eu), in the course of which the researchers attempted to access their own personal data on the basis of their rights guaranteed under the data protection laws in various countries, including Hungary.
procedure was more predictable, since it was quite easy to take the evolution of a single person’s quasi case law and extrapolate from that the position the ombudsman would likely take on certain questions. However, in a court case – both at a court of first instance and an appeal court – the decisions frequently diverged, even in similar cases. This resulted partly from the independence of the judiciary, partly from the acceptance or rejection of the evidence, but partly also from a slight degree of inexperience in data protection cases on the judges’ part. These factors, therefore, unequivocally speak in favour of the data protection ombudsman’s procedure.

On the other hand, a court decision is binding, while the data protection ombudsman’s decisions – at least in the initial period – were not mandatory, and even when that changed, his decisions could only be enforced to a limited degree in practice.

The legislators tried to keep the ombudsman’s procedure separate from the court procedure by offering these two paths to the data subjects as alternative courses of action. The data protection ombudsman was not entitled to act in those cases that either were being investigated in court or had already been adjudicated in a court of law. At the same time, an ongoing investigation by the data protection ombudsman did not limit the court’s authority, so those who wanted to exhaust both channels had to go about it in the right order: they first had to file a complaint with the data protection ombudsman, and only when that investigation was over could they turn to the court. Although the two investigations were independent from one another, the judge could be influenced by the professional opinion of the data protection ombudsman.

We must also briefly mention the role of the “fourth enforcement model” (self-regulation) in the execution of the data protection provisions. After the mid-1990s – following the enactment of the data protection act – a number of sector-specific acts were passed, which made it obligatory for each of the various organisations in the data protection sectors to draft their own internal data protection regulation, as well as to appoint an internal data protection officer. Naturally, the internal data protection regulations could not be in contradiction with the current laws, although they could define the actual content of their interpretation and enforcement in the practices of the various organisations dealing with processing of personal data. The 2003 amendment of the data protection act made it obligatory to prepare such regulations – and to appoint internal data protection officers – in a broad circle,

---

37 Given their training and practical work, the judges understandably display more competence in the traditional branches of law (civil law, criminal law, etc.) and have difficulty identifying with the approach more closely related to the fundamental rights laid down in the Constitution. In their arguments, they tend to rely on the civil code, rather than on the data protection law or the sector-specific provisions of data protection regulations. Only a small number of judges are conversant with information rights (even though the first data protection ombudsman had still made the effort to regularly organise joint professional consultations with representatives of the judiciary, with whom he discussed actual problems in the interpretation of the law).

38 Act LXIII of 1992, Section 24. a), Section 27 (1).

39 For example, the 1995 law on direct marketing or the 1997 law on data protection in health care.

40 See the data protection law in health care.
which prompted massive efforts in both drafting such regulations and launching training courses for the data protection officers.

In both areas, one can encounter numerous misunderstandings in the practices of data protection experts and advisors. In some parts, the regulations simply copied certain chapters of the data protection act, without containing the crux of the matter: the internal division of tasks, the responsibilities and the details of the data processing procedures. Some of the internal data protection officers were not quite clear about their own role: whether they were “moles” or “agents” sent out to report to the ombudsman on the internal irregularities or, quite the opposite, their job was to cover up the unlawful practices in their company’s data management so as to protect it from both the complaining data subjects and the data protection ombudsman. Naturally, it was neither: their actual task was to represent the interests of the organisation, while staying within the boundaries of the law. In other words, their job was to invent and apply data management processes, so as to enable their organisation to carry out its main task in an efficient (or in the business sector, profitable) manner, while obeying both the letter and the spirit of the data protection law. Privacy policies had already been available for the data subjects, and especially for the users of Internet services, as early as the 1990s, but a real proliferation in this regard took place in the first years of the new millennium. The quality and the content of these information materials varied vastly: some provided the data subjects with specific information, others only contained generalities, and some claimed things about the processing of personal data that were simply not true. Finally, there were those who only wished to win the confidence of the customers with some advertisement-type message. According to a survey conducted in 2005, in the case of a considerable number of Hungarian webpages, online privacy policies were either completely lacking or were incomplete; the most informative were the webpages of the Hungarian branches of international companies, although even these mostly contained texts translated from the parent company’s information leaflets, rather than locally relevant information.

4.5 Political changes and a new model in enforcing data protection

In 2010, 20 years after the democratic transition, Hungary witnessed some major changes, both in politics and in legislation. The political party that won an absolute majority at the parliamentary elections abolished the constitution, changed the official name of the country, dismissed a good part of the judiciary, limited the

---

41 Laszlo, Gabor, “Magyarorszagi weboldalak adatvedelmi nyilatkozatainak elemzese” [Analysis of privacy policies on Hungarian webpages], in Ivan Szekely and Mate D. Szabo (eds.), Szabad adatok, vedett adatok [Open data, protected data], BME GTK ITM, Budapest 2005, pp. 95–114.

42 This was replaced by a new Basic Law, designed for a similar purpose.

43 The designation “Republic” disappeared from the official name of the country.
authority of the constitutional court, placed the media under strong government influence, and introduced a centralised system of political leadership and institutional framework. The new leadership seriously weakened the constitutional framework that had previously been patterned on a western model, its institutional guarantees and system of checks and balances, and used its parliamentary majority to abolish or transform the organisations of the State, including the institution of parliamentary ombudsmen. In the course of this, it repealed the data protection act in force and summarily dismissed the incumbent data protection ombudsman as of 1 January 2012. The new political leadership basically denounced the democratic regime of the previous 20 years as illegitimate and, as a symbolic expression of this, it precluded the constitutional court’s decisions issued from legal precedence from being used as legal precedents. These incidents, along with many others, prompted the European Commission to launch accelerated infringement proceedings against Hungary in January 2012, which resulted in the Commission’s rebuking the ruling political elite for curbing the independence of the National Bank and the data protection authority as well as over the measures affecting the judiciary. The Venice Commission of the Council of Europe put forward similar criticisms on several occasions. In response to these admonishments, the political leadership was forced to introduce minor changes in the wording of the laws, but the previous status quo was not restored.

The 1992 data protection act was replaced with Act CXII of 2011, which, while preserving the cornerstones of the earlier law, strengthened the positions of the data controllers at the expense of the protection of data subjects, and replaced the institution of data protection ombudsman with a government body, the data protection authority, NAIH (Hungarian National Authority for Data Protection and Freedom of Information). To the superficial observer, the change may seem formal (especially in view of the fact that a former – more precisely, the second – data protection ombudsman, Attila Peterfalvi, was appointed as head of the new authority), even though the difference between the two supervisory bodies, the parliamentary ombudsman’s office and the data protection authority, is substantial. This is clearly shown in the text of the laws defining the mandates of the institutions: the data

---


46 In its April 2012 bulletin, the Committee announced that it had accepted the Hungarian responses in the area of the national bank as adequate, while in the case of the judiciary and the data protection authority, it upheld its criticism.

47 The European Commission for Democracy through Law – better known as the Venice Commission, as it meets in Venice – is the Council of Europe’s advisory body on constitutional matters. It provides legal advice to its Member States and, in particular, to help states wishing to bring their legal and institutional structures into line with European standards. http://www.venice.coe.int/WebForms/pages/?p=01_Presentation

48 http://www.academia.edu/1760582/The_Venice_Commissions_opinions_on_Hungary_and_the_Hungarian_Governments_responses_-_Summarising_table
protection ombudsman’s task is “to protect the rights and freedoms afforded by the Constitution for the protection of personal data and access to information of public interest”, while the new authority is responsible “to oversee and promote the enforcement of the rights to the protection of personal data and access to public information and information of public interest”. Phrasing it differently, the data protection ombudsman seems to be above codified law in the sense that he is responsible primarily for protecting fundamental rights and thus he can occasionally go against the legislation in force in the interest of protecting constitutional values, he is empowered to turn to the constitutional court, while the new authority is merely responsible for overseeing compliance with the provisions of the data protection laws.

These two institutions have different positions within the structure of the State: the data protection ombudsman was elected by Parliament, and was obliged to report to Parliament only, while the new authority is one among the many government offices, and its head is appointed by the Hungarian president at the recommendation of the prime minister. Although the independence of the new authority is nominally guaranteed under the new data protection law, his actual independence is questionable, especially in comparison with the independence of the data protection ombudsman’s office. The European Commission criticised the legislation related to the appointment and dismissal of the head of the new authority (these were later modified by the Hungarian political leadership), but even beside that, one can question the practical independence of the new authority in dealing with any improper data handling by other branches of government. – In this regard, we discuss below some ongoing independent research.

Naturally, the two institutions envisioned their own roles differently: the data protection ombudsman primarily relied on the powers of persuasion and public openness in enforcing his recommendations and decisions, while the NAIH prefers to operate through administrative fines and other forms of sanctions.

The question can be posed – leaving aside the changes in the political environment – whether it was really necessary to reform the institution of the data protection ombudsman, and what other options, beside establishing a government authority, would have been conceivable and feasible. While still in office, Andras Jori, the last data protection ombudsman, developed a concept, which would have renamed the ombudsman’s title as Information Commissioner and instead of the earlier method of financing – a joint budget with the other parliamentary ombudsmen – it would have had a separate budget, thus guaranteeing the institution’s full independence. Jori submitted the concept to the committee responsible for drafting

---

49 While we know of a number of supervisory authorities in long-established democracies that have managed to remain independent regardless of their integration into the government structure, in the case of the new democracies, there are several factors that can endanger the genuine independence of such agencies.

the Basic Law that came to replace the Constitution, but the committee made no use of it in its work.\textsuperscript{51}

Thus, while the new arrangement combines all three models of data protection enforcement, their relative strength, as well as the relationship between them, has shifted considerably. The main emphasis is on legal enforcement, even though the NAIH took over some of the tasks of its predecessor: it continues to have the power to make recommendations, both general and specific, to specific data controllers.\textsuperscript{52} The way to a court procedure in data protection cases is still open, although the separation between the new authority’s activities and the courts’ enforcement role is less clear now than it was earlier: in certain cases, the authority itself can turn to the court; it also has the power to intervene in court procedures initiated by others.\textsuperscript{53}

\section{4.6 Edifying cases}

It is too early to draw general conclusions from the authority’s track record after just 3 years, nevertheless, it appears that it is the mass-scale enforcement authority function that poses the most serious problems for the NAIH: it still has not been able to bring the data protection register up to date (this is the reason it has not collected the registration fee), and it cancelled the option of accessing the registry via the Internet – hopefully, only temporarily. Furthermore, the supervision of the standardised search and retrieval system for data of public interest has produced no visible result: although the interface of the web service has been updated, there has been no improvement in the compliance rate.

While the NAIH is not a legal successor of the data protection ombudsman’s institution, the new law on data protection obligates the new authority to take over from the data protection ombudsman’s office all of the cases still open at the time of switchover. We can best demonstrate the difference between the two institutions’ visions of their own roles by presenting cases that either spread across the switchover period or occurred in the practice of both institutions and had a similar character.

One of the cases the NAIH inherited from the data protection ombudsman concerned the data protection aspects of a populist campaign by the government taking power in 2010. As part of that campaign, the government circulated nationwide a questionnaire as a means of “national consultation”, which was designed to formally legitimise the government’s actions, to increase its popularity and to run a registry on the political preferences of the respondents. In the course of the 2011 campaign, these questionnaires were mailed to the country’s entire population as political

\textsuperscript{51} In the opinion of the author – who was among the founders of the institution of data protection ombudsman – the strengthening of the official powers would have been reconcilable with the role and parliamentary legitimiation of the ombudsman.

\textsuperscript{52} Act CXII of 2011, Section 38 (4) c).

\textsuperscript{53} Section 38 (3) d), e).
direct marketing, using the database of the central population registration office. Still in office at the time, the data protection ombudsman initiated a meeting with the authorities concerned before sending out the questionnaires, because in his opinion numerous infringements of the law had been committed in the handling of the data in connection with the campaign. The authorities ignored the ombudsman’s concerns and the campaign went ahead. Subsequently, the data protection ombudsman published a statement in June 2011 – thus executing its “soft” powers – in which he called on the authorities to cease the illegal processing of data, pointing out that the responses to the questionnaires could only be recorded in an anonymised manner, and they had to be destroyed after the act of recording. Since the authorities failed to comply fully with this request, the risk of linking the personal identification data to the recorded opinions continued to exist. At that point, the ombudsman, making full use of the powers vested in him, issued a decision ordering the destruction of the personal data related to the questionnaires and banning the creation of the database formed by personal data gathered for the purpose of direct mailing.

The authorities concerned decided to challenge the data protection ombudsman’s decision in court, but the court proceeding did not start until 2012, by which time the institution of the data protection ombudsman had been abolished – presumably in line with the intentions of the authorities. At the first session of the trial, it was the new data protection authority, NAIH, which represented the data protection ombudsman’s position, and the two authorities mutually agreed to terminate the proceedings with immediate effect. The NAIH passed a decision, in which it reversed the earlier decision of the data protection ombudsman, stating that the data of those respondents, who had indicated their consent to future communication in a signed agreement, did not have to be deleted (in ordering the destruction of all the data, the data protection ombudsman had objected to a different aspect of processing personal data). In addition to the diverging professional approaches, it was evident that the new authority did not wish to go against the government: it founded its entire professional argument on a single provision of law, thus forsaking the protection of the data subjects and offering instead a compromise solution to the government, as data controller, for the execution of its planned action.

---

54 For example, one of the sections enquired whether the pharmaceutical lobby should be brought down, because “they take billions out of people’s pockets”, while another asked whether education should be adjusted to the real demands of the economy, etc. A similar “national consultation” was conducted in May 2015 “on immigration and terrorism”.

55 Central Office for Public Administrative and Electronic Public Services (KEK KH).

56 [http://www.jogiforum.hu/hirek/25999](http://www.jogiforum.hu/hirek/25999) [in Hungarian].

57 Attila Peterfalvi, President of the NAIH, already demonstrated that he tends to offer a narrow interpretation of the law in a high-profile case back in the days when he was still data protection ombudsman, and that incident paradoxically earned him the Big Brother Award – the ironic title awarded by civil society actors to institutions or persons doing their best to erode people’s private lives. The case concerned the right of department stores to fit their changing rooms with cameras, which Peterfalvi defended as legal on the grounds that the customers had been informed about it.

58 When the government carried out a similar campaign in 2012, entitled as National Consultation, it had previously changed the law in order to make its actions legally unassailable. Nevertheless, in
It is worth comparing two very similar cases, one investigated by the data protection commissioner, the other by the new authority. In 1997, two journalists independently from one another approached the data protection ombudsman about gaining access to the scientific work of politicians as public figures. The journalists wanted to read the doctoral theses of leading politicians, including the incumbent prime minister, Gyula Horn, but the institutions holding the dissertations rejected their request. The data protection ombudsman stated that limiting the freedom of information can only be constitutionally justified if it is deemed necessary to ensure the realisation of another fundamental right. He determined that the right to read books in a library’s holding primarily belonged to the authorised users of the library (especially in the case of limited-access libraries of universities or university departments), but in view of the author’s being a well-known politician and public figure, this right can also be extended to persons outside the circle of membership.\(^{59}\)

In 2012, an applicant turned to the NAIH for an opinion concerning the possibility of getting access to the academic theses of various public figures, including the current and the previous prime ministers, according to press reports. In its response, the authority stated that “there are no legal regulations prescribing that the content of an academic thesis must be made accessible to anyone on the grounds that it qualifies as public data on account of its being in the public interest.” Therefore, in the authority’s opinion, a higher education institute had complete autonomy in deciding who can access the institution’s academic theses. In addition, the document pointed out that the politicians had written their dissertations before becoming public figures.\(^{60}\)

Although the reasoning of the NAIH contains legally valid elements (not to mention the fact that the 1997 petition was not simply about dissertations, but academic work in general, for which a legal requirement of public access was much easier to justify), it is clear that the data protection ombudsman had given priority to the information rights of the citizens, while the NAIH recognized the primacy of university autonomy.

As part of a recent research project, the NAIH’s financial penalty policy was investigated on the basis of the information published on the authority’s homepage. An analysis of the data has revealed that the NAIH’s official procedures ending with a decision very rarely concern data controllers associated with government or local government agencies, and this rate is even lower with regard to decisions establishing culpability. Incidentally, the non-private data controllers (among the few data controlling agencies rebuked) are mostly local governments, with only a few other

---


public authorities here and there. With regard to the fines levied, the data show that
the NAIH imposed heavier penalties on private data controllers than on data con-
trollers associated with public authorities, in terms of individual fines, the sum total
of the fines and the average figure.61 On the basis of this information, the researcher
has concluded that the constitutionally stated independence of the data protection
authority is no guarantee of its relative independence from the organisations it sup-
posedly supervises.62

4.7 Open questions

The European Commission initiated an infringement action in January 2012 in reac-
tion to Hungary’s abolishment of the institution of data protection ombudsman, but
it has failed to produce any result (the Hungarian authorities did not reverse their
decision). The Commission then filed a case at the European Court in Luxemburg
against Hungary for violating EU law. In December 2013, the Advocate General of
the European Court published his opinion on this issue, in which he advised the
Court to reprimand Hungary.63 In its judgment of 8 April 2014, the Court ruled that
by prematurely bringing to an end the term served by the supervisory authority for
the protection of personal data, Hungary has failed to fulfil its obligations under EU
law.64 The only consequence of the judgment was that the Hungarian government
offered an apology and financial compensation to the dismissed Commissioner for
his loss of salary, however, the abolished institution has not been restored.

Whether the new authority will be able to demonstrate a growing independence
in its future handling of governmental data controllers will be seen in the forthcom-
ing period. This will be judged from various high-profile cases, the authority’s state-
mements and role perception, as well as from the relevant statistical analyses. Even if
we only consider its narrowly interpreted tasks associated with its capacity as a
public authority, most notably the tasks of maintaining the data protection registry
and running the standardised search and retrieval system for public data, it is dou-
btful how it will be able to fulfil these in the future. How seriously data controllers
will take their obligations and how closely they will follow the instructions of the
authority, whether they comply with the tasks the law designates to them only in

61 During the first 31 months of the NAIH’s operation, only 5 % of the fines were levied on state
data controllers and 95 % on private organisations.
62 See Szabo, Mate D., and Fanny Hidvegi, “Ket itetlet es vegrehajtasuk” [Two judgments and their
enforcement], Fundamentum, Issue 4, 2014, pp. 69–82.
63 “Hungary violates EU law on ending data protection ombudsman’s contract, says European
hungary-violates-eu-law-on-ending-data-protection-ombudsmans-contract-says-european-court-
official/
64 Court of Justice of the European Union, Press Release No 53/14, Luxembourg, 8 April 2014,
application/pdf/2014-04/cp140053en.pdf
form or also in essence will depend on the authority’s successes in discharging these tasks, and nowhere more so than in the area of Internet services.

However, besides the data controlling organisations, the general public, too, has a legitimate interest in learning about the new authority. In early 2013, one year after its establishment, the new authority commissioned a public opinion poll entitled “The Public Conception of the Situation of Data Protection in Hungary”.\(^{65}\) According to the results of the survey based on personal interviews of 2,000 people, 31% of the Hungarian population had heard about the Hungarian National Authority for Data Protection and Freedom of Information, which was considerably less than the corresponding figure for the former data protection ombudsman (see Flash Eurobarometer 225). Six per cent of the respondents knew the head of the authority by name; this is similar to the last data protection ombudsman’s name recognition, but both fell far below the name recognition of the first ombudsman (23%).\(^{66}\) Only 5% of the respondents knew of the authority’s activities, according to their own assessment. It is worth noting that only three out of ten people were satisfied with the Hungarian regulation of data protection (29%) and freedom of information (31%).

These data show that the authority needs to expend more effort in informing the public about its activities, as most people have heard about the establishment of the new authority only in connection with the abolition of the data protection ombudsman’s office and the highly critical EU report that followed it. However, name recognition by itself is not enough: the organisation responsible for effective data protection also needs to win the respect of the general public. Due to its character, an authority is less sympathetic to the public and the data controllers than an ombudsman, so only time will tell how successful the new enforcement model of data protection, along with the institution representing it, will be in gaining the public’s trust.

### 4.8 Conclusions

Overall, the codification and enforcement of the data protection laws can be described as a success story in Hungary’s post-communist history. The incorporation of the right to privacy and data protection in the legal system and the self-regulatory documents was achieved in a proper measure in the first period of the democratic transition, along with the institution-building related to the enforcement of data protection laws. The recent political changes have transformed the system of institutions, changed the enforcement model of the data protection regime and modified its legal guarantees. In other words, with regard to enforcing privacy in


\(^{66}\) Laszlo Majtenyi’s subsequent public activities, in which constitutional issues and data protection cases have played a central role, probably also contributed to his greater recognition.
Hungary, the former model pupil among the new members of the community of democratic countries has become a problematic grown-up. However, even the combined effects of these changes have failed to destroy the framework and enforcement mechanisms of data protection law, and this can be viewed as one of the lasting results of the democratic transition of 1989.

Although the political, ideological and legal changes in Hungary form an unusual mix, which pushes the limits of the European system of values, the changes introduced in the type of data protection supervisory authority, and in its enforcement model, do not go against the general trend in Europe. While in the years during the democratic transition, the ideal – not only in the former satellite states of the Soviet Union – was a data protection supervisory institution of high legitimacy that contained elements of the ombudsman system, in recent years, the value of administrative powers has increased. This is understandable in the sense that the volume of personal data processing has increased by many orders of magnitude in the past decade, the associated technology and its monitoring possibilities have become more complex, while the data controllers – including the Internet superpowers – comply with the data protection law only formally, at best. This changed scenario calls for a more austere supervisory body with stronger administrative powers. In an indirect manner, this trend is reinforced by the institutional consequences of the legal separation of data protection from privacy in the Charter of Fundamental Rights of the European Union, as well as the EU’s planned reforms of the data protection system (including, among others, the mandatory co-operation between data protection agencies and the planned establishment of the European Data Protection Board). The change in the data protection model is not the central element in the judgment of the Court of Justice of the European Union cited above, not even the dubious relative independence of the new authority: it is the mode of dismissal of an incumbent data protection ombudsman that lies at the heart of the case. Having said that, the independence and the role perception of the ombudsman will be greatly missed in all future cases, when in the interest of the realization of fundamental rights the constitutional values would have to be defended even against legal regulations in force, or when in a high-profile case the ombudsman would have to turn to the population to give publicity to a case, or when he would have to mediate between partners in data management cases of strategic importance.

The Hungarian history of enforcing privacy and data protection provides numerous lessons for countries recently freed from dictatorial political and social systems and for the new democracies of the future. We have seen that the euphoria of democratic transition, along with the rising stature of new rights and freedoms, tends to be short-lived, therefore, permanent guarantees of the new information rights must be created, both at the legal and the institutional level, in this brief, initial period. And as for the legal guarantees of the rights, it is better to set them at a level that is higher than the minimum requirement of international standards, partly in order to set the norms high in a society freed from a dictatorial system, partly to anticipate their probable future erosion and to ensure that they remain at a reasonable level even after the attempts to limit them. To wait until large parts of the population demand the codification and realisation of these rights would be a serious mistake.
Nor is it useful to suggest that information rights are the luxury of developed countries and that a transition country has no resources for such luxury, because a new democracy will probably never reach the stage of socially interiorising the information rights. Furthermore, the country may not even reach the status of a developed country, because there is a strong interconnection between the implementation of information rights and welfare.\(^6^7\) The Hungarian example has clearly shown that the establishment of the legal system and the creation of the institutional system have been successful, but the social awareness and acceptance of the law has not been completed, which has made the task of the opposing forces easier.

Privacy and data protection are just two of the fundamental rights of crucial importance in the democratic establishments of the twenty-first century. Similar advice can be given in establishing and enforcing other rights and freedoms, although information rights require special attention. Compared to other fundamental rights, they are less visible and less tangible, while they provide the basic foundations for the realisation of other rights. Without free access to public information, no informed, participatory democracy can exist; without the protection of privacy, there can be no freedom of speech.

Hungary is a small country, which never belonged to the club of Europe’s great economic or political powers. This is not the reason why her political and legal experiments are important: rather, they are important, because they can serve as examples, both positive and negative, for European and non-European countries alike, and – with regard to the spread and threshold level of the shared European framework – for the European Union itself.\(^6^8\) If nothing else, this alone makes it worthwhile to watch closely the unfolding developments in the enforcement of privacy and data protection in Hungary.

References


\(^6^7\) See, for example, Darch, Colin, and Peter G. Underwood, _Freedom of Information and the Developing World. The Citizen, the State and Models of Openness_, Chandos Publishing, 2009.


Laszlo, Gabor, “Magyarorszagi weboldalak adatvedelmi nyilatkozatainak elemzese” [Analysis of privacy policies on Hungarian webpages], in Ivan Szekely and Mate D. Szabo (eds.), Szabad adatok, vedett adatok [Open data, protected data], BME GTK ITM, Budapest 2005, pp. 95–114.


Vasarhelyi, Maria, “Lattuk-e, hogy jon?” [Did we see it coming?], Jel-Kep, No. 3–4, 2010, pp. 91–97.