



Convergence & centralisation: a former DPA's point of view

András Jóri, former Data Protection and Freedom of Information Commissioner of Hungary, examines the journey towards convergence of data protection laws in Europe and the world, and how the current European landscape - with the differences in privacy cultures from one end of the continent to the other - accommodates this concept. Mr. Jóri also describes his position on the role of the European Data Protection Board when the new European Regulation comes into effect, and how harmonisation would be achievable and sustainable. Finally, he shares his thoughts on the challenges of striking a balance between data protection and freedom of information.

When looking at the future of privacy, there are three issues which need to be considered. Is there really a chance of convergence that can lead to a globally accepted regime? How should one view the trend of centralisation that is proposed by the new EU framework? And, finally, as a former Data Protection and Freedom of Information Commissioner, I know very well the conflict that exists between data protection and the interests of transparency/freedom of information. How can we tackle this issue in a manner which enables us to continue to rigorously enforce our data protection laws without harming the image of data protection, for example, by avoiding adverse effects, such as the building of unnecessary obstacles in the way of transparency?

Convergence

Data protection, as a tool for privacy protection, has gone through extraordinary development over the last few decades. It appeared in the 70s in Western Europe and was then adopted in Central Europe in the 90s after the collapse of communism. Today, we see the idea of data protection conquering Eastern Europe and the Balkans. Israel is now accepted as a country providing adequate protection. Canada, Australia and New Zealand have their own privacy regimes, which are mostly in line with the concept we call data protection in Europe. Parallel developments can be seen in Central and South America and South East Asia. And, while authors for many years have described '*American exceptionalism*' as a key element of the global picture, convergence is nowadays becoming the new buzzword. The bipartisan Kerry-McCain Commercial Bill of Rights Act, the reports by the Department of Commerce and the FTC calling for a new system of privacy protection in the US can be part of this new narrative; as well as the cases where the new EU framework builds upon and uses instruments invented in the US (such as privacy breach notification) or widely known and used on the other side of the Atlantic (privacy impact assessments).

While these trends provide grounds for a certain degree of optimism, we should not forget that merely having data protection acts in place is certainly not enough. Data protection functions as part of the legal system of a given country, and if the value that is placed on the rule of law deteriorates in a country, then the level of privacy protection may rapidly decrease as a result. One Eastern European country, where I

am currently active as a consultant, has a cutting edge data protection act which my local colleagues are rightfully proud of; however, if you want to marry someone in this country you have to take obligatory and humiliating sexually transmitted diseases tests. In this case, we can remain optimistic that the efforts of the local DPA and civil rights advocates will be able to change the whole privacy culture in the long term. However, we are seeing examples where, while legal regulations regarding data protection are still in place, the situation is swiftly deteriorating: last year the Government of a Central European country carried out a massive 'consultation' campaign which led to the unlawful processing of politically sensitive information of hundreds of thousands of citizens; while at the same time, its Ministry of Justice organised a posh conference, where delegates from all over Europe discussed cloud computing and privacy by design.

It seems to me that the culture of privacy is strikingly different in the Eastern and Western parts of our continent, and while I am usually rather enthusiastic about the use of new and inventive instruments of EU data protection law to address new challenges that are posed by the appearance of fantastic and now ubiquitous technologies, I see a sad picture when looking to the East. A divide in political cultures means a divide in privacy cultures as well: talks about creatively elaborated new principles are empty babble when in certain European countries data protection advocates have to fight for the basic rights and freedoms of citizens, while officers of the local DPAs are enjoying themselves at Brussels conferences devoted to the right of oblivion on social networking sites, much to the governments' liking. Data privacy



rules might show convergence; but let us not forget about the need for convergence when it comes to those rules of legal principles that represent the foundations of privacy protection all over the world.

Centralisation

With the new draft of the EU data protection framework published in early 2012, many critical voices are now being heard. Some fear that the powers of the new European Data Protection Board might breach the independence of Member State DPAs. We have to be aware that data protection laws are tools for protecting privacy; and privacy, primarily, is a matter of culture. While some countries, for example those in Scandinavia, have centuries-old traditions of openness, others draw the line between the public and the private sphere differently.

When the EU lawmakers constructed the Directive, it was intended as a harmonisation measure to prevent the distortion of the functioning of the internal market possibly stemming from the divergent levels of protection. It was not entirely successful: still today, even basic terms of data protection law are interpreted differently in Member States. This causes additional financial burden and costs for controllers. However, it also gives Member States room to maneuver to define the scope of privacy protection in line with their national privacy culture, using the concepts of data protection law.

The new draft Regulation would unquestionably bring greater harmonisation. Basic definitions would be the same, the set of legal grounds would be uniform across the EU, and sensitive issues as the transfer of personal data, would be fully harmonised. An impressive system, aimed at the uniform

interpretation of law, is also included in the draft: when there is a clear tendency of diverging interpretations of national DPAs that cause community-wide issues, the European Data Protection Board and the Commission would have the necessary powers to prevent adverse effects using the consistency mechanism.

Is this a breach of the independency of national DPAs? I do not think so. During the last few years, the EU data protection community has been facing challenges that can be tackled only at the EU level. I have personal experience about cases, where my position (as the Hungarian DPA) was weakened by press reports of diverging opinions of other national DPAs in Europe.

Sometimes, I had the feeling that some major controllers providing services throughout the continent were using the tactics of '*divide et impera*' deliberately against national DPAs. If this was the pattern of how European DPAs deal with global service providers, our credibility would be lost in the short term. That is why I welcome this kind of centralisation in the proposed regime. It is still important, however, that within the new framework Member States still have the opportunity to express their values when deciding about conflicts between privacy and transparency: the possibilities for adopting Member State rules and derogations in certain areas included in the draft Regulation may provide for such solutions.

As for the independence of DPAs, the Regulation sets out certain rules regarding the appointment and dismissal of data protection officials. In this regard, the current text might not go far enough: the provisions about independence still make it possible for creative governments to meddle with independent data protection

supervisors, in the context of alleged 'restructuring' of DPAs. In this regard, we might need more centralisation: in less developed political cultures only stringent rules and guarantees for independence might provide effective protection.

Therefore, we need centralisation to tackle the issues that require interpretation on an EU level, and this does not go against the principle of independence of national DPAs. What is more, even a higher level of centralisation is needed, which might provide DPAs operating in countries with less developed political cultures with more potential to be successful as privacy advocates.

Conflict with transparency

When I was elected Data Protection and Freedom of Information Commissioner in 2008, the image of data protection was seriously harmed in the country. This was a result of certain earlier decisions by the DPA that were viewed by the public, NGOs and certain professional groups as not being aware of transparency interests. To cite an infamous quote: 'According to our interpretation, there is no such thing as an investigative journalist -- one either publishes something that is lawful, or he is a step away from prison'. The DPA stood for blurring the faces of policemen on videos published in the press, while NGOs held that this data should be public as the persons involved were carrying out public tasks. Even such institutions as the Constitutional Court turned down freedom of information requests on the grounds of data protection. According to the Justices, a brief submitted to the Court was not to be disclosed to the requester, because it qualified as the personal data of the author. (This case was subject to court



proceedings: while domestic courts upheld the original decision, the European Court of Human Rights finally struck the balance between data protection and freedom of information in a different way, and held that this exaggerated interpretation of data protection law had violated the Convention). A similar phenomenon can be described as having taken place during previous years at EU level. In the case of Bavarian Lager, a beer distributor applied for the minutes of an official meeting attended by the officials of a Member State, the EU Commission, and industry representatives. The minutes were disclosed, but the names of certain persons present at the meeting had been deleted from the public version. At first instance, the General Court held that transparency interests overrode data protection interests in this case; however, according to the final judgment of the European Court of Justice, the original decision to withhold the data was right. (Remarkably, the European Data Protection Supervisor intervened in support of the requester.)

These tendencies harm data protection: not striking the right balance between privacy and transparency can ruin the public perception of data privacy regulation and can also endanger the effective protection of transparency interests. That is why I am a supporter of data protection and freedom of information regimes which are designed in a way that the regulations in the two areas reflect each other, and that is why I like the idea of supervisory bodies that have competencies in both fields (like in certain provinces of Canada, the UK, Germany (federal and lander level), Slovenia, etc.). In my opinion, these authorities have a

[T]he culture of privacy is strikingly different in the Eastern and Western parts of our continent, and while I am usually rather enthusiastic about the use of new and inventive instruments of EU data protection law to address new challenges [...], I see a sad picture when looking to the East

better chance of developing comprehensive interpretations of data protection and access to information laws, reflecting the values and choices of the society they are operating in.

András Jóri

Consultant and Former Data Protection and Freedom of Information Commissioner of Hungary