Data Protection in the Judiciary:
The Challenges for Modern Management

Budapest, 24 October 2013

Giovanni Buttarelli
Assistant European Data Protection Supervisor

Speaking points

1- Introductory remarks

Let me start with some comments which are also related to my background as a member of the national judiciary in Italy.

Today´s debate focuses on courts and communication, but with your permission I would like to first deal with the judicial approach to information in a general sense. Some comments I will make refer to the penal area but they can be easily applied, mutatis mutandis, to other judicial activities in the civil and administrative area.

The legal systems of the European countries are not homogeneous with regard to the organisation of the judiciary.

The "trias politica principle" is normally respected in our countries: at its core, the judiciary should be independent and autonomous from other powers.

However, this independence implies neither a total discretion nor a rigid dividing line for the judicial function. Moreover, several countries have foreseen checks and balances or connections between powers, including for the judiciary.

For example, central organs of the executive or legislative powers play a role in the organisation of supporting services for the courts and tribunals (and this is relevant for what I will say about the "controllership" of data processing).

2- Data protection for the judiciary?

My mission today is to focus on data protection, on how national and EU principles in this area may contribute to modern and efficient data management which respects fundamental rights and freedoms.

First, however, we need to address a preliminary question.

While independent, the judiciary is one of the branches of State in all countries.

Therefore, it shares and should respect many other values, principles, legal and ethical rules which are typical of the public sector.

The specific mission of magistrates and judges is to administer justice, with a view to ensure that the rights of the citizens are properly defended, protected and satisfied, and to prevent, detect and suppress criminal and other offences. In many cases duties and powers are exercised within a very critical framework, with limited resources and a high workload.

Does this require the judiciary to have its own rules on data protection, different from the common rules applied to other public administrations and private entities?

How much are these adjustments, specific provisions or derogations justified? In other words, from a data protection viewpoint, how much should the judicial powers and offices

be considered separate and different from, a Ministry, for example?

Answering these questions may be easier if we first analyse the EU legal framework.

The fundamental rights and freedoms of citizens as now laid out in the Lisbon Treaty and the Charter of Fundamental rights do not allow for discrimination, restrictions, derogations and adjustments for the judiciary if they are not necessary for the performance of its specific duties and powers. The high data protection standards should be applied to all public and private controllers.

Article 16 of the Treaty on the Functioning of the European Union gives everyone -including third country nationals- a right to data protection enforceable before a judge. It obliges the Council and European Parliament to establish a comprehensive data protection scheme on which they are currently working intensively on.

I´m pleased to note that last Monday´s vote by the LIBE Committee of the European Parliament is an important step towards stronger and more effective data protection in Europe. The result is a positive step for further progress.

The Lisbon Treaty has equipped the EU with a legally binding Charter of Fundamental Rights which in Article 8 contains a right to the protection of personal data, separate from the right to privacy.

3- FSJ area and e-Justice

The entry into force of the Lisbon Treaty has also given new political and legal impetus to the discussion on what the exchange of information in the EU and the Area of Freedom, Security and Justice should look like.

Exchanges of personal data are a crucial element for successfully building an effective Area of Freedom, Security and Justice.

Important dossiers are and will be under discussion at EU level, for instance, on e-Justice initiatives which rely heavily on the processing and exchange of personal data between entities based in different countries and which are subject to data protection rules. e-Justice started out as a tool mainly for making national legislation available in other EU countries

but it now relies on other projects involving a processing of personal data.

For instance, if we reflect for a second on the challenge to facilitate the interconnectivity of insolvency registers at EU level, we can immediately find specific difficulties such as: (i) the allocation of responsibilities on the portal and national registers (ii) automatic translation/accuracy, since e-Justice entails the exchange of information originally created in different languages.

Privacy (in the traditional sense of respect for private and family life) and data protection (in the modern sense of engineering personal information) are extremely relevant in promoting a better quality of data exchange.

Moreover, data protection should also be seen as a tool that facilitates successful interaction and mutual trust between judiciary and law enforcement.

Judiciary and law enforcement are interlinked, each in their respective sphere of competence. However, there is a need for a more balanced approach which would fully respect the powers of the judiciary and the critical role it pays in a society ruled by law.

The judiciary must be well informed and provided with all necessary information and elements to make fair decisions and act with full independence.

4- Data protection: a tool for an efficient judiciary

Where appropriate, cooperative support by data protection authorities is also useful. They should be involved in order to prevent data protection from hampering judicial activities.

There are many good examples in Member States of a fruitful relationship between the judiciary power and stringent laws on data protection.

Indeed, there are a number of cases where the involvement of a national data protection authority, through in-depth dialogue for example, has been favourable for both the police and the judiciary.

It is time for an organic and proactive discussion on the efficiency of dealing with information in judiciary activities throughout Europe.

We should be able to identify whether there are too few or too many law enforcement databases, how they are accessible at national or international level and whether they are useless databases in stagnant waters rather than dynamic tools.

Generally speaking, with regard to Europe, my personal point of view is that we have few really intelligent databases which are directly useful for the judiciary.

The fight against crime requires efficiency and rapidity. Judicial authorities do not always have efficient instruments at their disposal for the prevention and repression of crimes and other violations, at the level required for the increasing challenges.

However, if we accept this status quo we cannot make the mistake of ignoring the rights, freedoms and dignity of the European citizen.

Data protection is not an obstacle to an efficient judiciary.

Data protection is only one of the factors that can influence the collection and processing of good information in a police or a court/legal data file:

a) many other factors need to be taken into account when checking the quality of information being communicated to the wider public or exchanged for law enforcement purposes, including bureaucratic approaches, outdated rules on judicial cooperation, jealousies or even competition in promoting and implementing the exchange and lawful transfer of information at international level;

b) some information is available but not readily used or exchanged;

c) overlapping flows of similar information exist. Initiatives could be promoted to gather more up-to-date information - subject to impact assessments on fundamental rights and freedoms.

An intelligent and contemporary approach to data protection could be extremely helpful in finding the democratic legitimacy of a more efficient police data policy.

Privacy by design is one of the key principles of the EU reform. It could easily be applied to the judiciary as well.

Indeed, too much data sometimes results in too little information.

For instance, one might wrongly feel the need to collect data that is already available elsewhere.

When a new database or the processing of data is to be established, decisions taken about the centralised/decentralised architecture, the means of interconnectivity or the further use of data at international or national level are extremely relevant in data protection terms.

Secure access to highly sensitive databases via multi-service cards, management of biometric information, platforms to exchange selective genetic data where necessary, strong security measures adopted by the courts, access by citizens to court files, onsite inspections of IT systems are just some examples that make up the European and national scenario that I envisage in the coming years.

5- Food for thought - how to implement data protection principles

I see many members of the judiciary from various countries present here today and I encourage each of you to better and more concretely implement principles such as:

a) the principle of necessity (under which the use of personal and identification data shall be configured to minimise their processing if the purposes sought can be achieved by using anonymous or non-identifying information) and

b) the principle of transparency (under which any kind of processing of personal data must be transparent in accordance with the law).

We have no doubts about the need to reinforce the judiciary's management of data: however, not everything that is technically feasible is also socially acceptable, ethically admissible or legally permitted.

New technologies and new technical applications are both useful from this perspective.

Why not, for instance, implement the so called "*one box only"* principle, by storing data in just one place accessible to magistrates and judges subject to appropriate guarantees and to certain conditions and safeguards including the need-to-know- principle? In this case, lawful and fast access, traceable twice (once on communication and once on reception) may

help in preventing massive reproduction of data in several places, increase data quality and reduce security risks.

Why not appoint more privacy officers for court databases?

Why not encourage an effective implementation of privacy enhancing technologies (PETs) so that automatic tools might prevent certain breaches of data protection rules?

In consideration for the consequences for citizens, more efforts are also necessary to distinguish between data related to administrative data which must be retained to document the procedures and other more sensitive data concerning, for instance, criminal behaviours.

What can Europe and data protection contribute?

A lot! By investing in common training programmes, by creating additional networks for mutual exchanges and trying to achieve at European level what, in light of consolidated national situations, might be more difficult to achieve at Member State level.

As I already mentioned, the new data protection rules based on the renewed legal framework of the Lisbon Treaty

may also offer an important contribution and help overcome national difficulties and fragmentation.

For instance, there is an ongoing debate on the future role of large scale information systems centralised or coordinated at European level but accessible by national police authorities and, in some cases, by court authorities.

6- Data protection and communication

On a practical level, what needs to be done on a daily basis in order to give more substance to the principles of data protection, especially for communication purposes?

I will try to give some specific examples, which also stem from my personal experience of enforcement at European and national level.

In my opinion, it is important in data management to:

a) have a detailed and up-to-date snapshot of the databases and of the most important categories of data processing;

b) identify and allocate responsibilities in a precise manner, and comply with the procedures necessary for

ensuring that these activities are kept under control, making it possible to implement the appropriate solutions as and when required, particularly in cases of data breaches. This is especially important for databases that are shared by several courts or investigating bodies, or that are managed by a central administration such as a Ministry or self-governing body, even though they can be accessed by peripheral users. In these cases, it is vital to identify all controllers and processors, even for cloud computing services;

c) better distinguish between activities that are essentially administrative in nature (to be in principle considered along the same lines as other activities of non-judiciary public bodies) and activities that have a direct bearing on the judicial function, the so-called *'jus dicere'* (for which some exceptions or modifications concerning data protection may be justified);

d) pay particular attention to sensitive data (as identified by the Strasbourg Convention and by European Directive No 95/46/EC) in all its various forms, such as data relating to minors and to family law, and biometric and genetic data.

The heads of courts and the judges presiding over cases or databases must pay specific attention to these problems, and

not delegate their macro-management to administrative personnel: these are critical legal issues.

Further problems also arise from the proportionality principle and from the balancing act that the courts must perform when communicating data externally.

Here, one of the main problems stems from the difficulty of applying the code of criminal, civil or administrative procedure that is relevant to the case whilst at the same time also protecting data.

Many national codes were drawn up long before the modern-day notion of data protection came into being, and although they contain some provisions relating indirectly to privacy, they focus only on procedural matters in the strict sense, rather than on respecting individual rights.

At the same time, while many national data protection laws in theory apply to procedural matters, whether in full or in part, this is far from the reality, or at least, cannot readily be perceived by judicial staff.

In addition, it may be the case that national laws do not contain any specific exceptions, rules or adjustments relating to jurisdiction, and this too could further complicate matters.

For instance, 41 of the 46 Countries to have ratified Convention No 108/1981 state that they apply it within their judicial offices, while only 5 of them state that they do not apply it to certain judiciary matters relating to the prevention of crimes or the management of databases on criminal proceedings. How do all 46 countries apply the Convention, for example, in civil proceedings?

Moreover, following the Amsterdam and Lisbon Treaties, it can reasonably be considered that the European Directive is applicable to civil and administrative judicial matters: how many of the Member States are currently aware of this in regard to their own internal regulations, pending the approval of the European reform of data protection rules?

Just as traditional procedural codes were not drawn up with data protection in mind, national data protection laws are also at times 'horizontal' and are not always scrutinised so as to be effectively applicable to the judiciary (such as the right to access information that an interested party has on the data relating to them).

This requires specific, innovative efforts from those tasked with applying the principles of data protection in the courtroom.

There are several areas, such as the storage of data over time, in which there is still much work to be done in order to reduce any factors that are irrelevant to the ultimate objective: we cannot consider that all data should be stored indefinitely just because court activities need to be documented to the n^{th} degree.

As regards other aspects such as external communication and access to documents, we must embrace new technologies and be similarly creative:

1) measures should be initiated in every country to check whether the procedural standards in place are relevant to the issues that we face today, and to better distinguish who is qualified to have the right to access case files and data, and for what specific purpose (parties to proceedings, interested third parties). For journalists, historians, researchers or statisticians, there is much tension across Europe concerning the application of the rules that allow access to anyone 'who has an interest';

2) those who draw up decisions that can be accessed by third parties should pay close attention to what is vital for a proper and comprehensively reasoned statement, omitting any superfluous detail;

3) in many countries, procedural matters are increasingly based on computer and IT technologies. Careful attention must therefore be paid when allowing the parties or their representatives access to the entire case file or to data identifying other pending disputes in which they are not involved, or to only the file of the proceedings in which they are already involved or have a qualified interest to access;

4) the decisions handed down by every judicial authority must be transparent and readily accessible, and also be published on the website of the judicial authority itself. However, some common sense should also be applied, given that such decisions are often also published in online legal journals;

5) consequently, the parties to the proceedings (and third parties) should be able to access a transparent mechanism in order to prevent certain sensitive data relating to minors, family issues, violence, etc. from being exposed not by the

original decision, but rather by any copies made accessible. The procedural judge should be able to assess the reasons of the parties, of third parties and also of the court;

6) broadly speaking, sentences and other decisions published on the Internet should not be revealed by search engines external to the website, but instead remain searchable only through internal search engines.

7- Conclusions

The administration of justice often takes place under extremely difficult circumstances. However, criminal, civil and administrative courts are not ‘free from areas’ where the respect of individual rights such as privacy, personal identity and dignity can be put aside.

On the contrary, data protection, in its current form goes beyond the mere protection of privacy and is a prerequisite for handling such sensitive issues effectively and with public confidence.

This is why, in conclusion, I encourage all those involved in the data protection debate to consider and to understand the need for an intelligent and contemporary data protection policy.

I am confident that we can all support a new generation of data protection rules comprised of more substance than redundant formalities,, of concrete guarantees rather than abstract reminders of general principles that are not respected.

New user friendly, technically advanced, concrete and unbureaucratic rules are to be promoted.

Greater justice for citizens requires increased data protection.

Thank you for your attention.