LEGAL INFORMATICS AND THE SCARCITY OF JUSTICE

Ahti Saarenpää

Professor Emeritus, Institute for Law and Informatics, Faculty of Law, University of Lapland
Lecturer, Faculty of Law, University of Helsinki, Vice Chair, Data Protection Board
Member, Finnish Academy of Science and Letters
Yliopistonkatu 8, 96300 Rovaniemi, FI
ahti.saarenpaa@ulapland.fi

Keywords: ***Network Society, Data Protection, Reading Law, TeachingLlaw, Social Science***

Abstract: *In the general classification of sciences, law is ordinarily considered one of the social sciences. This comes as a surprise to many practitioners. We are used to thinking that our discipline is somehow distinctive – a science that studies justice. What we know as ordinary legal doctrine, our guide to interpreting the law, has little or no interest in society or its development.*
In the Network Society, we will inevitably see more regulation on the relationship between law and technology – even though our ambition is to produce technologically neutral laws. Having more regulation on the books will heighten the role of ordinary legal doctrine. At the same time this development should alert us to the increasing importance of legal informatics as a modern social science. Data protection is a premier example of this status. We simply cannot afford to overlook its links to human and fundamental rights in the constitutional state.
I put forward the argument that today general legal science is a more important social science than ever before and that it will play an increasingly crucial role in how we interpret the law day in and day out.

1. A leading case

September 2017 the Finnish media were abuzz with the breaking news that the *National Institute for Health and Welfare* placed the health data of over 6'000 people on an information network, the Internet. The leak was not discovered by the Institute; they found out about it from the national Data Protection Ombudsman. One citizen had alarmed his office to the breach.

When the Institute ultimately made a public statement about the incident – over a month after it happened – the reason given was merely «human error». One of the people working there had used information containing personal identity codes when putting together a report. They then, without thinking about it, put the information on an open network.

Sadly this incident reveals the vulnerability of our society more generally, dependent as it is on information systems and information networks. Unintentional and deliberate violations of information security, as well as various leaks, now occur routinely, almost daily. It was with this in mind that the new European General Data Protection Regulation (GDPR) took as one point of departure that *data breaches* must be reported immediately, within 72 hours. But a lot can happen in 72 hours, far too much.

I won't be going into any further detail on the Finnish incident, but I think there are a least three observations merit mentioning here. First, the data protection legislation prescribes that when processing personal data, every effort should be made to avoid processing unessential data. This means avoiding the use of identifying data that could be exploited by unauthorized parties. More often than not, the case or file number is a better identifier that the ever-risky personal identity code. These guidelines must be kept in mind when planning an

information system; those *designing the systems* have to consider the entire path the information will take in its lifetime.

Secondly, information systems should always be planned to minimize the risk of human error and the impacts of such error if it occurs. This clearly had not been done in the case I have just described. Some «dummy» managed to make a major mistake because there were no safeguards in place in the system that would prevent such errors or alert users to potential problems.[1]

Thirdly, I would point out that *information security* is a core value in the Network Society. Conscious of this, back in 1997, in a report drawn up by the Institute for Law and Informatics at the University of Lapland, we proposed that a general information security act was needed in Finland. At the time, the government did not find such legislation necessary, however, and to this day there is no such law on the books, regrettably. Fortunately, European regulation – on both data protection and information networks – has begun to take information security more seriously. It is one of the most essential forms of *security in a society*.

Following these short observations, I would like to go on to examine shortly the connections between information technology and law – *LegalTech* – on a more general level, drawing on the example of the protection and regulation of personal data.

2. Forward- and backward-looking sciences

We have become accustomed to thinking that the discipline of law – one of the skill sets that have become a science – is counted among the humanities rather than the (hard) sciences. It is quite distant from the technical sciences. It is so far removed from them in fact that communication between the technical and legal professions is sometimes quite difficult indeed.[2] This is a classic case that, like many others, bears out the first part of Wiio's Law, coined by Finnish professor Osmo A. Wiio: «Communication generally fails; when it succeeds, this is usually by accident.»[3]

The range of lawyers out there today is a very broad and diverse one. There are those who fear technology and those who prefer to avoid the legal issues connected with it. Then again, there are also lawyers who welcome technological development enthusiastically as a new object of regulation. In that zeal, however, many fail to realize that nothing is created in a vacuum. Everything has its background influences – legal influences among them.

Yet another group can be identified – unfortunately – consisting of lawyers who, working outside case law systems sit back waiting for court rulings on the relation between law and technology. This group, by no means a small one, which seeks out and slavishly follows these decisions, is not always a credit to the legal profession. The development of society and technology might very well pass them by – to their peril and ours too.

As a rule, law and lawyers practically work by combining *normative* and *factual premises*. In assessing facts we often encounter something new; in assessing norms we look for materials to aid in interpretation, with these then mostly offering something old, telling us what has happened and what leguslators have been thinking. Trying to draw conclusions on these bases thus involves a temporal tension. Law and its practices can be considered backward-looking activities. Ordinary law – normal science – is above all a *backward-looking sci-*

[1] The Finnish *Act on Openness in Government Activities* obligates those operating in the public sector to train users of information systems to give due consideration to the principle of openness and its limits. Unfortunately, in many places, this requirement is no more than a dead letter.

[2] See for example BUDD Research in the Two Cultures: The Nature of Scholarship in the Humanities pp 1–21 in Collection Management 1989.

[3] Professor Wiio (1918–2013) was internationally one of those few researchers who understood that we were taking the first steps toward the Network Society already at the beginning of the 1970s.

ence. It should thus come as no surprise that encounters with new technology sometimes result in considerable difficulties.

Against this backdrop it will be interesting to take a look at the development of personal data protection as a legal phenomenon and as a facet of the teaching of law.[4]

3. Data protection in legal perspective

On of the central elements of *ethics* for a long time – a very long time in fact – has been *privacy*. In normative terms, we have a right or rights to be alone. The old English maxim «My home is my castle» reflects this principle quite aptly. Privacy has long been protected through a variety of laws. And it has been protected without using the word «privacy» as a general term. In recent times, the expression, adopted in the United States in the late 19th century, and later its counterpart in Europe, «private life», have become established more or less universally to describe what is an *individual human right*. In one development reflecting the legal significance of privacy in the robustly evolving constitutional state, the UN now has a Special Rapporteur of the Right to Privacy, first appointed in 2015. Our privacy in society is becoming increasingly important.

The heightened status of privacy as a human and fundamental right reflects a change in the conception of the state. In most countries on the globe a gradual transition has been made – or is underway – from the *administrative state*, which controlled and monitored its citizens, to the *constitutional state*, which shows higher regard for the individual. Put briefly, the latter is a state where the rights of the individual vis-à-vis society are stronger than before and are realized earlier in all legal relationships. Citizens are now guaranteed justice long before the fair trial, which was once the flagship of the constitutional state.[5]

In Europe the early seventies saw links emerging between privacy and the protection of personal data. Memories of the Second World War and the increased calculating capacity of computers were seen as a combination that deserved more attention from the legislator. Sweden had the distinction, in 1973, of being the first nation to enact a Personal Data Act – *data lag* – that applied to the whole country[6]. Detracting somewhat from this distinction, given how we see things today, is that the law was enacted largely out of a fear that information technology would be abused. In fact, for a time creating a computerized personal data file in Sweden required a permit. This reflected the strong Nordic administrative state at work.

The 1995 European *Personal Data Directive* has been the cornerstone of data protection in Europe for a good two decades. Its twenty years of application have changed the legal landscape in our field quite a bit. We now also see a greatly changed society and state – and use different language for talking about them.

From the legal point of view the drafting of the *European Charter of Fundamental Rights* ushered in a new era. The Charter sets out the fundamental rights approved by the European Union. They represent crucial elements in the development of the modern European constitutional state. Adding to their weight is the Charters strongly binding prohibition on the abuse of rights, embodied in its Article 54, a provision designed to avoid incorrect interpretations of the law. The Charter separates privacy and the protection of personal data. *They are distinct fundamental rights*. The protection of personal data – unlike in the Anglo-Saxon conceptual world – is no longer merely a facet of privacy. It is nothing less than *a fundamental right in and of itself*.

---

4 The author is vice chair of Finland's highest data protection authority, the *Data Protection Board*. The present two-tier system of oversight will be discontinued when the Regulation comes into force. Finland will establish a Data Protection Authority, to be led by the Data Protection Ombudsman.

5 I am not referring here to what is known as *proactive law*, which is a narrow interest of its own in the discipline.

6 In this connection, it merits mention that the German state of Hesse had already enacted its own state-specific Data Protection Act and that this matter was discussed elsewhere as well. Accordingly, in Finland, drafting that had already begun was discontinued in 1974 due to political differences. The political Right wanted relatively minimal protection for people's right of self-determination; the Left sought more extensive regulation of society's information flows.

The same change can now be seen in the European General Data Protection Regulation (GDPR), which came into force in 2016 and becomes applicable as of May 2018. The Regulation does not mention privacy. It protects all of our fundamental rights and especially the right to personal data protection. Although it does not mention privacy in so many words, it of course protects privacy too. After all, privacy is a fundamental right in itself, and more often than not protecting personal data serves to protect privacy as well.

But the change here is not merely a matter of semantics; far from it. At its core lie a concern for daily routines and a desire to relieve people of what has been a constant search for the boundaries of privacy. When thinking about the legality of processing personal data, it is no longer necessary or possible to deliberate how private the data are. The Regulation's point of departure on this issue is wholly different: it will – with certain exceptions – always be applicable when we *process personal data*. And the concept of personal data in the Regulation is a broad one, covering a very wide range indeed of data: identifying data, communications data, and data relating to the personal aspects of a natural person. This, I dare say, is what we can really call «data». The narrow interpretation of «personal data», often seen in practice, runs counter to today's conception of our fundamental rights.

4. Information systems in Society

We are making – or actually have largely completed – the transition into the *Network Society*, a society where we live and work in a digital environment that is dependent on information systems and networks. Our society today works and communicates quite differently than the one we lived in before the transition.[7]

Information systems play a crucial role in this new society. Where development in days past was assessed by measuring the degree to which various operations were computerized, today the focus is on how well information systems function – or how badly, as the case may be. The key questions here are *quality* and *permissible ways of using the systems*. The old excuses – that there are no bug-free programs or that delays are no surprise when running new software – no longer fly well in the constitutional state. Information systems and their use must be *designed* such that our rights are realized as quickly, unequivocally and comprehensively as possible. In the same vein, where malfunctions occur – and they do – systems must have rapid and effective technical and legal *resilience*; that is, it is essential to ensure that they recover from malfunctions robustly.[8]

What this means on the ground, for the profession, is that working as we do – and must – in the digital environment of the Network Society has rendered us legal *cyborgs.* We are utterly reliant on information systems and information networks. The design and use of such systems, especially those containing critical legal and administrative information, must be legally sound.[9] It is with this in mind that in the literature I have spoken of *digital lawyers* in the constitutional state. Good lawyers today are necessarily digital lawyers. There are no two ways about this in the modern constitutional state.[10]

It is essential that we proceed from this realization to consider how we, engaged as we are in teaching and research in the field, can promote the knowledge and skills digital lawyers require. I will continue with an example involving the protection of personal data.

---

7 See more for example Saarenpää, Introduction, in Saarenpää / Wiatrowski (eds.), Society Trapped in the Network – Does it have a Future? (2016), pp. 15.

8 About resilience see more for example Lucini, What is Resilience? The State of the Art, in Lucini (ed.), Disaster Recilience from a Sociological Perspective (2014), pp. 31–53.

9 «Data protection by design» used in the GDPR is a relatively new term but an old idea. It is one of the underpinnings of the modern history of regulation on personal data protection. Authors do not seem to remain aware of this when they milk the term for all it is worth in the literature.

10 See Saarenpää,The Digital Lawyer. What skills are required of the lawyer in the Network Society?, in Schweighofer/Kummer/Hötzendorfer (eds.), Kooperation / Co-operation, Tagungsband des 18. Internationalen Rechtsinformatik Symposions IRIS 2015 (2015), pp 73–85.

5. Legal systematics and the protection of personal data

Systematics plays a key role in legal life. It opens and closes the eyes; lawyers eyes. The general taxonomic location of a law in the legal system, along with the legal principles, theories and concepts that inform the law, tell us what is right in any given situation. As professor Aulis Aarnio, one of my teachers aptly wrote: «If systematic boundaries are violated, the decision made does not comply with valid law.»[11]

When Finland's first data protection law – the Personal Data File Act – was enacted in 1987, the editor of the systematic law collection *Suomen laki* (*The Laws of Finland*) classified it under *administration law*. There it was between the Bladed Weapon Act and the Bingo Decree. *Bingo!*

Three factors can be seen as leading to this old misleading classification. First, the Act was drafted in the Administrative Law Division of the Ministry of Justice. Secondly, in Sweden, the pioneer of such regulation, the legislation was seen as falling under administrative law – hardly surprising given that in 1987 the administrative state was still going strong. Thirdly, the editor had no established conception to draw on that would indicate what category data protection belonged to in the Finnish legal systematics. The editor was not familiar with *the law of personality* or with *legal informatics* as legal disciplines. Anyone opening the law book would end up with an incomplete picture of how significant personal data protection is. The so-called «open the law book» method was giving misleading results.[12]

Later data protection legislation found a systematic home in our law book as one part of the *Law of personality.* And it is still there between the Equality Act and the Names Act. Our systematics says a great deal about our values. And when we consider that *The Laws of Finland* is a collection of statutes intended for practitioners in particular, the work is also a key component of communication in and about law.

I myself teach data protection as a part of the *Law of personality* (Persönlichkeitsrecht) and a part *of information law*. We can and we should speak of *dynamic systematics*. By this I mean that, in addition to the basic system, we need specialized research skills in personal data protection in different impact areas. An illustrative and timely example is *public law*. Although the values underpinning personal data protection lie essentially in the rights of the individual, in particular the right of *self-determination*, we cannot skirt the need to have a sound understanding of the principle of *openness*. The new GDPR makes this very clear too. Its article 86 reflects the problems associated with the «unholy marriage» between the protection of personal data and the principle of openness. Standing in contrast to consistent protection of personal data is the inconsistent European public law where regulation varies from country to country:

> «*Article 86 Processing and public access to official documents*
>
> *Personal data in official documents held by a public authority or a public body or a private body for the performance of a task carried out in the public interest may be disclosed by the authority or body in accordance with Union or Member State law to which the public authority or body is subject in order to reconcile public access to official documents with the right to the protection of personal data pursuant to this Regulation.*»

In fact, the old European idea of *legal informatics institutes* is partly based on this very view too. An institute is an *interdisciplinary forum* for discussion within law as well as discussion directed to those outside the discipline. At the same time, it is the core of a dynamic systematics. Bringing the protection of personal data, privacy and openness together successfully under one roof, as it were, requires very wide-ranging understanding. This being the case, it has been and continues to be very difficult scientifically to justify legal informatics being a subject that can be tackled by a single researcher only. As individuals, we easily become *prisoners of the scarcity of justice*. Here we can see why the idea of establishing institutes for legal informatics in our

[11] Aarnio, Essays on the Doctrinal Study of Law. Springer. New York 2011 pp. 179.

[12] This perceptive expression was developed by Kauko Wikström, a Finnish professor. It refers to practicing lawyers whose information retrieval skills are essentially limited to consulting collections of statutes.

multifaceted Network Society is timelier than ever. If the legal community network is to operate effectively, it will need more than the traditional, static systematics and narrow scope legal skills.

6. Conclusion

Every legal culture and every faculty of law has its own distinctive way of *teaching law*. We might even speak of faculty-specific legal systematics when reading law. The freedom of teaching and research we enjoy makes this possible. Where courses with a relatively narrow focus are concerned, this variability is usually not a problem. In such cases, we are educating students specializing in preparation for a career in which they may later become experts in a very narrow field. However the links to legal method and theory are important there too.

But *legal informatics* is more, much more than a narrow specialization.[13] It is far from any narrow specilization. The discipline, if any, is a modern *social science* where the path information takes from creation to archiving or erasure is paved, as it were, with *fundamental rights*. The information infrastructure is a crucial societal framework for digital operations, one whose legal regulation is a challenging task indeed,[14] All of that is extremely important from a social point of view.

An essential facet of our science today is how we learn to address new technology and the opportunities it brings. The general doctrines of our field are more salient than ever before in the Network Society. If we fail to observe them, justice in practice will become increasingly scarce, with fateful consequences or at least ruinous delays.

I would like to take up one more insightful example, the well-known *Google Spain* case. At issue was our right to remain beyond the reach of search engines, beyond indexing. In deliberating the case, the court concluded that the protection of personal data was a more important consideration than freedom of speech. Ultimately, the latter was not even mentioned in the court's decision. We must be careful not to heedlessly take thinking rooted in fundamental rights beyond existing regulation. Similarly, law, as a modern science, must not forget the limits of the constitutional state. When speaking of the Information Society from the point of view of the social sciences this tends especially earlier often to be forgotten.[15]

Lastly, I would like to note that old-fashioned information technology and old-fashioned lawyers without methodological skills are a very bad combination where the rights of the individual are concerned. This is worth bearing in mind in any course of education or training, whether its focus is law, government and information technology.[16] In the next corner the scarcity of justice may be waiting for you.

---

13 Saarenpää, Legal informatics today – the view from the university of Lapland, in Saarenpää/Sztobryn (eds.), Lawyers in the Media Society (2016), pp. 10–16.

14 Bob Frankston has observed aptly: «An interface is best when it disappears and the user can focus on the problem at hand. In the same way, infrastructure is best when it can be assumed and becomes invisible». It is essential to add that in the Network Society the legal framework for the information infrastructure must not remain invisible or fall outide the realm of societal discussion. See Frankston, Preface, in Belli (ed.), Community connectivity: building the Internet from scratch (2016), p. 9.

15 See for example the interesting and important Information society books of David Lyon and Frank Webster.

16 See Saarenpää, Does Legal Informatics have a method in the new Network Society, in Saarenpää/Wiatrowski (eds., Society Trapped in the Network – Does it have a Future? (2016), pp. 51–75.