WESTFÄLISCHE WILHELMS-UNIVERSITÄT
Institut für Informations-, Telekommunikations- und Medienrecht (ITM)
- Zivilrechtliche Abteilung -
Prof. Dr. Thomas Hoeren

Leonardo-Campus 9
D-48149 Münster
Tel.: +49/2 51/83-3 86 00
Fax: +49/2 51/83-3 86 01
Email:
hoeren@uni-muenster.de

21. Juni 2012

Priority List for IMMI

IMMI includes a lot of various legislative plans. In my view is therefore necessary to built up a priority plan regarding the implementation of IMMI into law. The following items contain a priority ranking (No. 1 being the easiest tool to be changed). The text only contains very broad pre-ideas; further research is definitely needed to define the relevant legislative changes.

1. Data retention
   So far as I know, the Icelandic telecommunication act includes a very broad regulation regarding data retention which obliges telecommunications provider to store the data for six months. According to my knowledge, this provision has not been used in practise. The provision can therefore be acknowledged without any big controversy.

2. Interpretation rules for judges in cases of libel tourism
   Some elements of the IMMI plans do not necessarily need new statutes, but a clear interpretation of existing laws by judges. The problem of libel tourism protection might also be solved by a guideline. The problem has already been involved within the Lugano treaty which contains an ordre public rule. Cases like the British libel cases (super-injuctions etc.) should simply not be enforced in Iceland. This can be clarified in interpretive guideline for the judges. Problems still arise if Iceland adheres to the EU; but this problem cannot be solved by a statutory change.

3. History Protection
   A more complex issue is the history protection. The limiting period for the enforcement of libel cases can be decided by judges according to civil procedure law. Especially in the case of injunctions the judges usually decide about the necessity of an injunction on the basis of a case to case analysis regarding the expired time between the infringing act and

the start of the lawsuit. Therefore it is sufficient to start IMMI with interpretive rules for the judges including the principle that injunctions must be filed within two months after the internet publication. If that is regarded politically as insufficient the civil procedure law in Iceland can be changed including the two month rule.
The same applies to the principal of a maximum damage of 10.000 Euro. This is a principle which has nothing to do with civil procedure law but with normal civil law. It can be ruled by a non statutory interpretation guideline for judges or by a small change within the civil act. However it has then to be clarify, whether the maximum damage of 10.000 Euro is attributed for a "single case" means. In my view, it is furthermore unclear whether the limit is really enforceable as 10000 Euro is a very low amount of compensation in relation to i.e. extreme violations of personality rights.

4. Liability issues
IMMI mentions the problem of the liability of telecommunication networks and internet hosting providers. Regarding the EU Ecommerce Directive, it is true that the exception for general court orders without further definition is worrying. Iceland can try to race his voice in the existing discussion on the evaluation of the E-Commerce directive in Brussels. It might as well plan a new national liability regime which clearly states that telecommunication network providers are not liable for any access problems. Internet hosting providers should be held liable only in cases where they obviously know that a hosted website is illegal and nevertheless maintain the website. Thus, an easy liability regime might be drafted like

   (1) Providers shall be responsible in accordance with general laws for their own content which they make available for use.

   (2) Providers shall not be responsible for any third-party content which they make available for use unless they have knowledge of such content, the content is obviously illegal and the providers are technically able and can reasonably be expected to block the use of such content.

   (3) Providers shall not be responsible for any third-party content to which they only provide access. The automatic and temporary storage of third-party content due to user request shall be considered as providing access as well as a weblink.

   The model is based upon the considerations of the Advocate General Jääskinen at the ECJ in the case L´Oreal ./. ebay (9 December 2010)
   http://curia.europa.eu/jcms/upload/docs/application/pdf/2010-12/cp100119en.pdf

   Furthermore it reduces the liability of host providers to cases with obviously illegal content applying thus a principle of traditional press law (liability of publishers for third-party content) to internet law.

5. Whistle blowing and freedom of information act

Whistle blowing is a topic which is really complicated to regulate. We don't have too many regulations in the world regarding whistle blowing. Whistle blowing concerns a lot of data protection issues so that the balance between whistle blowing and data protection needs further clarification. The priority of this important topic is to be regarded as not to high as Iceland should wait for the EU-discussion on whistle blowing and data protection.

6. Cloud computing

   In my view one of the most striking features of IMMI was the focus on cloud computing. This topic is very important and might help Iceland to be one of the big cloud computing countries in the world. Iceland has a perfect climate for big IT centres. It might invite foreign cloud computing providers to come to Iceland (for instance by a reasonable tax reduction). The cloud computing provider might get a kind of Icelandic quality seal if the company stick to data protection rules according to the EU standards. For instance, the tax reduction and perhaps an exclusion from any liability regarding stored content might be granted if the cloud company (processor) sticks to the rules of the German Data Protection Act (Sect., 11).

(2) The processor shall be chosen carefully, with special attention to the suitability of the technical and organizational measures applied by the processor. The work to be carried out by the processor shall be specified in writing, including in particular the following:

1. the subject and duration of the work to be carried out,
2. the extent, type and purpose of the intended collection, processing or use of data, the type of data and category of data subjects,
3. the technical and organizational measures to be taken under Section 9,
4. the rectification, erasure and blocking of data,
5. any right to issue subcontracts,
6. the controller's rights to monitor and the processor's corresponding obligations to accept and cooperate,
7. violations by the processor or its employees of provisions to protect personal data or of the terms specified by the controller which are subject to the obligation to notify,
8. the extent of the controller's authority to issue instructions to the processor,
9. the return of data storage media and the erasure of data recorded by the processor after the work has been carried out.

The controller shall verify compliance with the technical and organizational measures taken by the processor before data processing begins and regularly thereafter. The result shall be documented.

(3) The processor may collect, process or use the data only as instructed by the controller. If the processor believes that an instruction by the controller violates this Act or other data protection provisions, the processor shall inform the controller of this immediately.