dr. Géza Tényi:

RFID and privacy – present and future regulatory issues

Abstract

In the last year the role and regulation of RFID became an important topic of the European Union's policy. This paper will shortly focus on the privacy issues, as the most important factor in the regulation and social acceptance of RFID. After examining the current legislation, the most important regulatory issues will be highlighted, pointed out where the classical definitions and functioning of the data protection regulation cannot fulfil they role in the case of RFID. After identifying the crucial regulatory issues, the author holds up the regulatory measure to be taken. Finishing the analysis a conclusion will be drawn for the future regulatory aspects for the forthcoming technological development.

RFID from a privacy lawyers view, fundamental rights, effective regulation

There are several aspects of legal problems by entering of a relative new developed technology in the everyday praxis. A very important question is always to examine which kind of impact will the new technology have on our privacy? If the legal order, the protection of personal data faces new challenges, will be able to find the right answers, the right solution of the threats? If not, which kind of regulatory activity could be helpful, is a modification of the legal order adequate or a new specific regulation has to be made? And finally, can these regulatory activities lead us to change our regulatory paradigm?

Technological progress and privacy

It sounds like a cliché to go over the old ground again, that the regulation of data protection aims at achieving free movement of personal data and parallel protection of privacy, where a balance between these two values shall be created. Securing the free movement of personal data is important to secure economic and social progress, so to say the competitiveness of the internal market; on the other hand privacy means the core element of human life and also constitutes the basis for other fundamental rights and freedoms. Balancing between these very important values is always a hard task, where the initiation of confidence is always a key-issue.

There is a widely spread and nearly evident opinion, that the regulation of data protection was actually an answer to the fears from the rush development of informatics in the 1960's, where the confidence had to be restored to such institutions and organisations, which using this kind of technologies. While in the 1960s state's organs and their relatively backward technology were a subject for the regulation, nowadays it covers the whole society and data protection is facing the uprising technologies.

Therefore the fear from new effective technologies threatening our privacy provides a permanent issue for the regulator, which can be solved through flexible, technology neutral, general regulation, as we see in the General Data Protection Directive. Although the technical and economic development of the last years creates a need on regulation because of the new groups of personal data and special processing demands.

There is a new technological development in the fields of informatics for what we have to give our attention, the so called "ubiquitous computing" or "pervasive computing" or "ambient intelligence". On the level of definitions there is a technical development in two directions, informatics became mobile and parallel to this there are traditional informatics, which became omnipresent, in fact omnipotent. If we combine these two directions, we reach the level of the so called "ubiquitous computing". It means therefore a technology able to be present in any area of the human life, which means a huge advantage to make our life more comfortable and our activities more effective, it also can serve security or identification reasons, in some cases total control of a given area. In an extreme case the human individual could be the Unknown Soldier on the IT Front.

At this point we should avoid the infinite debate between the privacy groups and the supporters of new technologies and

the fact has to be accepted, that RFID and the forthcoming new technologies gain more space in the everyday use, although without the consumers "active consent", i.e. the practical acceptance this developments they cannot be successful. Therefore the traditional balance of private and business interests shall be protected in the future, for what reason data protection regulation in force has to be examined whether it is able to meet these requirements effectively. There are few specified issues as changing the basic concept of personal data, consent of the data subject, purpose of data processing, informational duties and role of the data commissioner, which shall be examined in the following paragraphs.

New categories of personal data

The RFID technologies are applied in several situations, where in most part of the present cases the application does not mean the collection and processing of personal data as logistics. These cases are not relevant and are outside of the scope of the data protection regulation, too.
Beside of the above the application of RFID technologies is gaining more space in the field of electronic identification and some business models where personal data will "directly or indirectly" processed.
In cases of direct processing the aim is to identify the client or the employee, to ensure special business benefits both for the consumer and the companies, or to give access to special restricted areas for trusted personal. In those kinds of cases the processing of personal data is based on a special agreement, where the data subject gave his consent, or furthermore the data processing is based on a labour contract. In that cases data processing is well founded, the purpose-bound nature and the duration of the processing leave some open questions, which can be regulated on the base of general data protection regulation.
More important is the "indirect" processing of personal data, where personal aspect of some data is not evident in any cases. Article 2 of the general Data Protection Directive defines personal data as any information relating to an identified or identifiable natural person, where the natural person can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. The Hungarian Act on Protection of Personal Data and Access to Data of Public Interest defines it more precise in its Article 2, i.e. 'personal data' shall mean any data relating to a specific, identified or identifiable natural person as well as any conclusion with respect to the data subject which can be inferred from such data. In the course of data processing such data shall be considered to remain personal as long as their relation to the data subject can be restored.
In this connection there is an 'indirect' processing of personal data, where the connection between a natural person and the given commercial good can be restored, the natural person can be identified throughout and the data processing of any commercial good in an RFID system can lead to an unexpected processing of a person-connected data. In a normal business environment this kind of information can be used for creating user profiles, but in several cases can lead to unwanted, unexpected processing of personal data. This secondary effect can therefore causing problems for companies using RFID technologies and proofs that the classical regulatory conclusion based on an expending definition of personal data can lead to practical problems.

Purpose of data processing, consent of the data subject, informational rights

Basically the usage of RFID technology serves the development of better service conditions, the exercise of contractual rights and more precise allocation of supply. Because of the indirect nature of such data mentioned above, there will be always a huge interest and temptation-factor for such companies to reach over the original scope of the data processing both in time and data categories to create a detailed user profile on the basis of a normal contract.
There is also another special character of the application of RFID technologies. The Data Protection Directive and all of the Member States Data Protection Acts provides that data processing fundamentally can occur if the data

subject has unambiguously given his consent, which can be given also through concluding action. In the case of complex RFID applications there is no reasonable solution to give the consumers a possibility to declare their opinion about the eventual processing of personal data.
There are several rights ensured by the Data Protection Directive for the data subject to control processing of his personal data. In the RFID environment, were data processing is not visible and traceable, these rights are loosing their importance, in most of the cases they are practically not applicable anymore.
These phenomena effect, that the general rules of data protection in this environment, where the classical rules of perception and control are not valid anymore, cannot be appropriate applied and the protection of the individual through legal system in force is getting restraint in this area and new legislative measures has to be taken. Therefore the question arises, whether the amendments of the general data protection rules or a specific regulation in this field can provide a solution for the problems above.

Regulatory issues: specific regulation or specific clauses in the general regulation

These crucial point mentioned before indicate a need of regulatory action, which restores the level of the personal data protection in that area. In the data protection regulation a high number of specific regulations can be found besides the general rules. There is a special segment of the applicable RFID technology, where the general data protection rules have to be applied, in absence of sector specific regulation. In the European data protection law is a specific regulation beneath the General Data Protection Directive for the data protection regulation of the electronic communication, the ePrivacy Directive. This specific Directive is part of the Regulatory Framework for Electronic Communications, thus the above data protection rules are applicable only to the public communications network. Here we are facing the same problem, why the European Union made a specific regulation for the electronic communications, i.e. the increasing capacity for automated storage and processing of data.
The ePrivacy Directive as a specific data protection regulation is based on the fact, that the public communication networks are a special segment, where new advanced digital technologies are currently being used in the Community, which give rise to specific requirements concerning the protection of personal data and privacy of the user. These digital networks have large capacities and possibilities for processing personal data, where successful development of these services is partly dependent on the confidence of users that their privacy will not be at risk.
The RFID technology means also the same kind of challenge to the privacy of the individuals, although it is not a special segment as the public telecommunication, the relating technologies are more separated and do not build an integrate network. The rules of the ePrivacy Directive cannot be applied for the problems mentioned above, because the RFID technologies doesn't function in the public telecommunication networks, instead of this they use private telecommunication networks with no open access and no services for the public. Therefore there is no need for specific regulation, the regulatory aspects of the RFID technologies can and shall be solved in the frame of the general data protection regulation.

Present regulatory issues on RFID

By that point of technological development there are several specific questions, which need to be answered by virtue of the amendment of the general rules of data protection. These questions are on the consent of the data subject, moreover on informational rights, the shorter period of data processing and storing, and the new role of the data protection authorities regarding the preventive control of the developments in the field.
The question of data subject's consent is combined with the information rights, for the reason that without any prior information the data subject is not in the situation to decide. Therefore the scope of preliminary informational duties of the data processor has to be expanded and this

duties shall take effect right at the beginning of the RFID covered area, to inform the data subject about his concluding consent with the entering of the given area. Although this new informational duty wouldn't make the classical informational rights and duties unnecessary, the data processing company shall take this obligation as a proportional burden for the economical advantages brought them by the technology.

The strengthening of the informational duties in itself gives only the basis for the rebalancing of the data subject and data processor relations. Moreover due to the enhanced data processing technology there is no reason and purpose to accept a longer processing and storing phase. Therefore the legal regulation should contain also specific rules on the shorter storing period and earlier deleting obligation as a consequence of the stronger enforced purpose bounding.

Last but not least in full consciousness of the new technological threats the position of the data commissioners has to be strengthened. There is already the possibility for prior checking through the data commissioners in case of the application of new technical data processing technologies at data controllers. According to Article 28 of the Data Protection Directive each Member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive. In consideration of the threats of the RFID technology and their bad reputation through the consumers, the prior checking possibility should be developed to a prior authorizing power for the data commissioner securing the publicity for the whole process.

Summarizing the proposals above the data protection legislation in force should be amended, where the informational duties and the purpose bound nature of data processing should be strengthened, the processing and storing period should be shorter and the data commissioner shall take the power of prior authorization in every new RFID application project.

Future regulatory steps, RFID regulation as a pilot project

As it was mentioned RFID is both a present regulatory issue and a forerunner of new, intensive intruding technologies. If we only look at the development in the last 3-4 years of this area, we can see an unexpected technological development and a very dynamic acceptance in the global business.

The technology, which is nowadays a passive application for identifying goods and natural persons, in the forthcoming years will gain more and more efficiency and flexibility, furthermore to act as the personal computers today.

Accordingly it is also a realistic expectation, that the regulation of the application of RFID technology will be an appropriate example for the forthcoming regulation of forthcoming technologies. The regulation cannot be prepared to every technological challenges, therefore the flexibility of the general provision is a very important value to prefer.

The regulatory example of the RFID technologies gives two basic principles for the future regulation. First, the advantageous position of data processing companies shall be compensate at the data subjects through various obligation for the data controller and checking possibilities for the data subjects. On the other hand the position of data protection authorities shall be strengthening, to preserve their controlling position.

The fundamental idea of data protection regulation is the balance between the economical interest and protection of privacy, where the change of this paradigm is not expected. The new technological developments shall lead us to rethink the checks and balances in the system to preserve the original paradigm.

Geza Tenyi
research fellow

Centre for Infocommunications Law
Institute for Legal Studies
Hungarian Academy of Sciences
Orszaghaz 30
1014 Budapest
+36-30-456-9341
geza.tenyi@ijc.hu
http://www.ijc.hu