# Road tolling and privacy. Some comments with regard to the EC Directive on Data Protection

Lerouge, Jean-Francois

*Published in:*
Computer Law and Security Report

*Publication date:*
1999

*Document Version*
Publisher's PDF, also known as Version of record

# DATA PROTECTION — TRANSPORT

## ROAD TOLLING AND PRIVACY

### SOME COMMENTS WITH REGARD TO THE EC DIRECTIVE ON DATA PROTECTION[1]

*Jean-François Lerouge*

**Jean François Lerouge examines how proposals for an automatic road tolling system in Europe might conform to the requirements of the EU Data Protection Directive. He also considers the adequacy of these rules in the road tolling context.**

## INTRODUCTION

Nowadays almost all European countries are confronted with the problem of traffic congestion. Many consortia are devoted to such a subject and many solutions are put forward in order to try to improve mobility inside European countries. One of the recurrent solutions is to require the user to pay for using the road. The tolling solution is considered as a great help for the purpose of curbing the demand and should encourage people to use public transport.

Some Member States have adopted a tolling system for a long time. Others, such as England,[2] intend to install one. There are different possibilities to organize the tolling on the roads. It is, however, very important that traffic not slow down due to payment requirements. Therefore, the actual objective of many countries consists in promoting an automatic system designed to avoid traffic congestion where users have to pay.

It is recommended that any new system should comply with basic requirements. So, for example, any system may, in the future, have to comply with some European requirements established by forthcoming legislation on tarification.[3] An automatic tolling system should also use common technical features to permit the driver to use the same system in any country, in order to facilitate better mobility inside Europe and avoid new obstacles to fluid traffic within Europe. It also needs particular measures to warrant that payment has occurred (contractual objective), to pursue fraud and to permit the debt recovery (repressing objective). All this will probably induce the operators to use technical systems (generally a flash of the registration plate),[4] to identify the driver although a good distance opening barrier may already be satisfactory to avoid fraud.

Regarding the above requirements, many projects of automatic tolling have already been experimented upon.[5] Each of them renders possible the collection of numerous data that will probably be exchanged between European countries (date, place, time and amount of payment, number of kilometers realized, when, on what road...). Such data will not only serve to demonstrate payment (contractual use) but could also be used for statistical purposes, controlling the traffic and detecting infraction to the highway code (policy use), or the monitoring of an employee by an employer or a wife by a jealous husband, etc. Fortunately, in its Communication,[6] the Commission clearly insists on the fact that any decision regarding tolling systems should be adopted in conformity with the general principle of the information technology and the EC Directive on the *Protection of individuals with regard to the processing of personal data and on the free movement of such data.*[7] There are many projects already tested. It is impossible to analyse each of them in spite of their evident interest.[8] In this contribution, it is proposed to examine three different, already tested, EU projects, and to see how an automatic tolling system could be used in conformity with the directive and whether or not such directive offers sufficient protection of the individual. It will highlight the necessity to adopt common legislation and will make recommendations for its adoption.

## PRESENTATION OF THE PROJECTS ANALYSED

### The Mans Project

The Mans project is a project initiated by the four Nordic countries (Norway, Sweden, Denmark and Finland). On the basis of their experiences, they have established common guidelines and recommendations on interoperable road user fee collection to be implemented in each of the countries' national legislation. This means that the guidelines, enabling interoperability, will be included in the legal concessions which regulate how the toll road operators should design their payment systems.

One of the preliminary recommendations on interoperable road user charging during the experimentation period of such project, was to maintain the possibility of a deferred payment as a main payment option and/or as a way of exception handling. In the context of this analysis, we will hereafter associate the Mans project with the idea of deferred payment.[9]

### Project Based on the use of Smart Card

Many projects are based on the use of the smart card. One example is Adept II. Adept II is an EU 4th framework project. Here the technology involved the use of smart cards and


ISSN 0267 3649/99/$20.00 

microwave-based transponders. In this project, the electronic chip of the smart card contained a transport purse, a link to a central account, public transport pass and a log file.

For the purpose of this analysis, when referring to Adept II, we will consider, as an alternative, the hypothesis of the use of a smart card without a link to a central account even though this was not the purpose of the Adept II project.

## Technology for Automatic Account Identification

Another technology has also been tested: *the Technology for Automatic Account Identification.*

A payment system based on Automatic Account Identification (AAI) is built on radio communication between in-vehicle equipment and roadside mounted equipment. The basic principle is that the vehicle communicates a string of information to the roadside equipment. The strings identify an account where the fee will be debited for future invoicing. This account is stored in a central computer system, which is updated at fixed intervals. One could go further and imagine the same system but with satellite technology locating the vehicle instead of roadside equipment.[10] The reader is now familiarized with the projects that will serve as a basis for this analysis. The next point will be devoted to the legal rules which apply in the field of data protection and privacy and to the problems that may occur regarding the tolling systems as presented.

## ROAD TOLLING AND THE EC DIRECTIVE ON DATA PROTECTION

The European Directive on the protection of individuals with regard to the processing of personal data and of the free movement of such data was adopted on 24 October 1995. The text lays down a number of principles with regard to the protection of fundamental rights and freedom of natural persons and, in particular, their right to privacy with respect to the processing of personal data. The Directive pursued a dual objective: ensuring the free flow of personal data within the Union whilst at the same time establishing common rules safeguarding the fundamental rights and freedom of individuals.[11] The member states were required to transpose these principles into their national legislation before 24 October 1998.

It is not the aim here to analyse each national law[12] for the purpose of seeing if the decision to install an automatic tolling system would comply with data protection legislation. The Directive offers common criteria for such analysis. By studying the Directive, one would like to see whether the current European legislation allows such installation and on what conditions. One should also try to determine which system seems most responsive to privacy and data protection criteria. Finally, we will see if there is any need for new EC legislation for the use of such systems. Prudence is, however, recommended in the interpretation of the conclusions we may draw. As Professor Poullet points out,[13] Recital 9 of the Directive highlights the importance of the "margin of manoeuvrability" enjoyed by the Member States. In addition to this there is the traditional margin of interpretation of the wording. Therefore for any conclusions that may be drawn with regard to the directive, this does not necessarily mean that the same conclusions can be drawn with regard to national legislation. As far as possible we will attempt to draw the attention of the reader whenever a different interpretation may be possible between the legislation of Member States.

The first section will be devoted to an identification of the personal data that may be collected with the automatic tolling solution. We will also briefly have a closer look at the notion of "processing of personal data". Secondly, we will identify the "controller(s)". Finally, we will identify the obligations that the controller must respect. We will see that some of them are problematic with regard to what we are dealing with.

## Personal data collected and their processing

Following article 2a, Personal data shall mean: "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified directly or indirectly, in particular by reference to an identification number or to one or more factors specific to their physical, physiological, mental, economic, cultural or social identity". Article 2b of the directive offers a definition of the processing of personal data: *"Processing of personal data shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use disclosure by transmission, dissemination or otherwise making available, alignment, combination, blocking, erasure or destruction."*

Those definitions adopted are very broad. The latest one seems all-encompassing. By reading those articles, some conclusions may already be drawn. Let us first point out that the notion of information is not defined. In application of the Directive (it may be different for some member states), it is not necessary that the information should comply with some particular formality. A written, coded piece of information or one present in a sound or a picture makes personal data.[14] Following this, in case of automatic tolling systems, the following personal data may be considered as potentially processed:

### 1. Data collected *a priori*

Some data may be collected on the subscription agreement any, for example when a toll badge is granted.[15]

### 2. Data generated or created through the use of the telematic system

By the use of the system, a number of data may be collected such as:

- the registration number plates in case a flash of the registration plate is used (whatever the purpose, eg. proof or repressing of fraud);
- the date, place, time and amount of the payment;
- the number of kilometres realized, when, and on what road.

A problem may occur when a car, registered in the name of a legal entity is flashed when crossing the tolling place or when an employee pays with a card of a company in application of the technical system of Adept II or when the payment system is based on Automatic Account Identification (AAI). According to the Directive, legal persons are outside its scope of application. However: "if data related to a natural person (e.g. the name of a director of a company) is present amongst information related to a legal person, then the directive applies."[16] In specie, the question is to know whether or not the person is identifiable according to the registration number of the company's plate or the transaction realized by the reloaded smart card or in application of the AAI technology (is the account where the fee will be debited for future invoicing, in the employee's name?). The application of the directive will in fact depend on the interpretation of the criteria used to determine if the person is "identifiable". The Directive states that " an identifiable natural person is one who can be identified directly or indirectly, in particular by reference to an identification number or to one or more factors...". Following recital §26 of the Directive for determining whether a person is, or is not, identifiable, account should be taken of all the means which might reasonably be used by the controller, or by any other person to identify such a person.[17] The identifiable character appears here to be taken into consideration with regard to the possibilities of the identification the controller(s) may have.[18] Here, we may thus be faced with data we may consider as anonymous regarding the physical person because it may require an excessive effort in terms of people, time and money to associate the data with a natural person. Therefore, on the question of knowing whether or not the Directive will apply when the data collected corresponds to the data relating to legal entity, one should assess whether or not the factual circumstances surrounding the identification of the individual requires an unreasonable amount of effort on the controller's part. According to this view, it is on the controller's liability to prove that a datum is not identifiable.[19] One should know, however, that some member states do not agree with this view.[20]

This issue may appear quite theoretical but in reality it seems important to point out that in the example, legal persons will not necessarily fall outside the scope of application of the Directive. This should avoid the creation of a specific system only for business use.[21]

## The Controller

According to article 2 d of the directive, the controller is the natural or legal person who alone or jointly with others, determines the purposes and means of the processing of personal data. When the purposes and means are defined by laws or regulations, the controller may be designated by such law.

In application of the definition, one may identify different persons for the tolling system who will be considered as Controller:

- the operators as regards the processing of the data concerning the use of the road;
- the bank, when there is a link between the smart card and a central account (for example in the project Adept II in the case of reloaded card[22] or following the technical AAI) with regard to the payment information and the information generated by the payment;
- in another context, the registration plate office. Indeed, as has already been explained, in the case of automatic tolling systems, many operators will flash the registration plate for the purpose of avoiding fraud or simply to conserve proof of the driver's passage in the case of any payment dispute.[23] The operators will be interested in identifying the link between the person and his/her registration plate. To establish such a link they will seek information from the registration plate office. Therefore, if the latter communicates such information to the operators, it will be for another purpose than one purely relating to the prosecution of criminal offences or tax collection. This reminds one that the legitimacy of such communication by a public authority should be examined with regard to the Recommendation n°R (91) 10 of the Comite of Ministers[24] article 7 e and f of the Directive[25] and therefore be foreseen by law.[26]

Some of those actors (i.e. the bank on the registration office...) may already be considered as controller for other specific purposes. They may individually be considered as Controller depending on the role they might play in the determination of the purposes and means of the processing of personal data. In addition, some actors, such as the bank, could be interested in creating a shared system of information and, with the operator jointly considered as Controller. In fact, the system in place may be quite complex linking both controller and processor.[27]

To have the same controller operating in all European countries, no other possibility seems to exist than imposing, by Directive, the same actors.[28]

## The controller's obligations

Hereafter we will identify the most relevant obligations that the controller has to comply with, with regard to the collection and the processing of data when crossing the tolling place.

### 1. To obtain the consent of data subject or processing necessary for a specific purpose

According to article 7 of the Directive, *Member States shall provide that personal data may be processed only if:*

*(a) the data subject has unambiguously given his consent; or*

*(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or (...)*

*(c) (...)*

*(d) (...)*

*(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or*

*(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of*

*the data subject which require protection under Article 1.*

In what follows, each of the conditions that have been identified as relevant for this case will be analysed. The choice of one criterion instead of another will depend on the forms of relations between the public entities, the owners of the networks and infrastructure on the one hand and technological operators on the other.

### a) The Data subject's consent

The data subject's consent is defined as any *freely* given *specific* and *informed* indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.[29]

Each element of the definition will now be considered and the practical effects explained:

- *any given indication of his wishes*
  The form of the consent is not important. The consent may be written or oral. It may be general (except in application of the exception provided by the Directive[30]) or implicit, i.e. in this case, the consent may be deduced by the use of the road. One could indeed consider that the driver, by using the road and the automatic tolling system, has implicitly agreed that its data be processed by the operators.
- *a freely given consent*
  The data subject's consent must not be given under pressure (which may be particularly difficult when an employee uses a company car). It notably implies that there are no consequences of discrimination if the consent is not obtained. Although one must recognize that compliance with such a condition is difficult to verify, which therefore renders it theoretical,[31] one should also point out the importance and the difficulty of respecting such a condition in the case of automatic tolling systems. Therefore, for economic reasons, there is concern that some Member States, not yet having any tolling systems may decide to install only an automatic one, which could offer the driver no other alternative than acceptance of the processing of his/her personal data.[32] In this case, one may consider that his/her consent has not been given freely, that no processing is thus authorized and therefore that such an automatic tolling system is not allowed.
- *a specific consent*
  The data subject's consent must relate to a particular purpose. The consent must relate to a well-defined and legitimate purpose. Use of vague or generic finalities must therefore be avoided.[33] In other words, the data subject must know exactly what is the extent of his given consent. In specie, the data should only be collected for the purpose of permitting the payment and the billing if any, and eventually the traffic management. Any broader given consent should not be taken into consideration.
- *an informed consent*
  The consent of the data subject must be informed. In other words, the data subject must be made aware of the risks and advantages of the processing and must be informed of his rights before consenting to the processing of his data or the conclusion of a contract that may involve a necessary processing of data. This implies that the controller must inform the data subject of these.[34] In specie, it is difficult to imagine any other possibility to inform the driver than give him the relevant information when he concludes the contract with the operators,[35] or at the time the driver receives his tolling card or his transponder. Moreover, the contract should necessarily contain information about the identity of the controller in all European countries, and the right of access of the data subject.[36] A piece of information given by a board placed along the road seems largely inappropriate since it is given after the implicit consent of the driver.

It is clear that there may be problems with regard to the data subject's consent. This, however, does not necessarily mean that the controller will not be authorized to collect and process personal data. Article 7 provides alternatives to the obligation of obtaining the consent of the data subject.

### b) A processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller

The term 'public interest' varies among Member States. Similarly the expression 'exercise of an official authority' is difficult to define in the abstract. Whether or not the activity is carried out in the exercise of an official authority will depend on the circumstances of the case. With regard to this, it may depend on the link existing between the public authority and the operators; in short in identifying the actors involved in the tolling road project and the context of their intervention (request of the public authority, margin of manoeuvre...). Recital 58 of the Directive, which gives examples of public interest in the cases of international transfers of data between tax or customs administrations, is not clear enough for drawing firm conclusions. If one looks at the European case law, it is interesting to point out that part of public interest objective is to realize an optimal road network.[37] One must, however, draw the attention of the reader to the fact that the notion of an *optimal road network* is rather broad and that a consensus on such a notion may be difficult to obtain. But, in the present case, as already explained, European countries are notably trying to encourage mobility,[38] to avoid traffic congestion and reinforce security on the roads. It is notorious that they look for the best service to offer to the user in the best economical circumstances. The European Union thinks that IT may play a significant role in achieving such a purpose.[39] It cannot be denied that all of this seems relevant to the public interest. Therefore, it is submitted that, if the system is organized as a result of the adoption of a specific law (and not by a decision of a European consortium of private operators),[40] the data processing could be based on such provision. Such a law should be common to all European member states which seems unavoidable since article 14 foresees a right of objection from the data subject otherwise provided by national legislation.[41] The law will, however, still have to fulfil the criterium of legitimate purpose.[42]

### c) A processing necessary for the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed

Article 7f states that personal data may also be processed if the processing is necessary for the purposes of the legitimate

interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under article 1.

Recital 30 of the Directive provides help for the understanding of this article that seems very broad and a danger for a person who would like to avoid the necessity to obtain the consent of the data subject. Following recital 30: *"in order to be lawful, the processing of personal data must be necessary (...) for the legitimate interests of a natural person, provided that the interests or the rights of freedoms of the data subject are not overriding; (...) Member States may similarly specify the conditions under which personal data may be disclosed to a third party for the purposes of marketing whether carried out commercially or by a charitable organization or by any other organization or foundation, of a political nature for example, subject to the provisions allowing a data subject to object to the processing of data regarding him, at no cost and without having to state his reasons."* The philosophy of this recital (notably, the data subject's right of objection)[43] promotes us to think *a priori* that it is not useful as a basis for a right of processing. The analysis in the following section of the criterium of legitimacy will confirm this.

Following this, a first conclusion may already be drawn: according to article 7 of the Directive, the right to process personal data seems finally to be conditioned by the adoption of a law on the basis of public interest.

## 2. Collect data for specified, explicit and legitimate purposes

Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.[44] Moreover, personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed.[45] It is a matter of limiting *a priori* the scope of infringement to privacy by fixing the borders of the controller's action. The specified purpose should also permit the control of processing's legitimacy and the pertinence of the data by the control authority.[46] The legitimacy of the purpose is easily understandable: individual liberty and rights may not be violated without any justification. The purpose of the processing should therefore be useful and necessary with regard to the corporate purpose of the company or its general interest. The criterium of legitimacy is also used in Article 5b of the Council of Europe Convention for the protection of individuals with regard to the automatic processing of personal data.[47]

Further help for interpretation may be found in article 8§2 of the Convention for the Protection of Human Rights[48] and in the case law of the European Court of Human Rights. According to the latter this is only acceptable as an attack on privacy if the attack is sufficient and pertinent.[49] Let us see by a concrete example taken from French case law of the CNIL, (the French authority in charge of privacy control) what are the exact conditions mentioned in Article 8 of the Convention.

### *a) Description of the case*

In 1996, the Société des autoroutes Bas-Rhin (SAPR) brought a particularly interesting file before the CNIL.[50] The SAPR wanted to experiment with an automatic reading plate system for vehicles moving on its AutoRoute. In such systems, the "traffic captors" permit the identification of a vehicle in a traffic flow. Data so collected have to be retained for a month in an indirectly nominative form, then made anonymous for statistical reasons. The CNIL, basing its reasoning on Article 8 of the Convention, judged that such a project, founded on the identification of all vehicles using a motorway network at a given time, attacked privacy and the fundamental right of persons to move anonymously. The CNIL also insisted on the limited rule of the operators ruling that they were not in charge of policy development. The latest point is interesting given the fact that in another case,[51] the CNIL accepted the reading and processing of registration plates by customs officers.[52] This begs the question of whether or not a flash of the registration plate made for the purpose of controlling fraud when crossing the tolling place should be considered, as the French authorities did, as being contrary to the fundamental right of privacy.

### *b) Analysis of Article 8*

Article 8 states that: *"everyone has the right to respect for his private and family life, his home and his correspondence. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the Law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection for health or morals, or for the protection of rights and freedom of others."*

This Article raises the following question: what might happen in the case of interference made by a private person or company (i.e. a private tolling operator) since this Article seems only to refer to *public authority*. If Pettiti[53] is correct referring to the *A.c. France* case,[54] it seems that the interference must necessarily be made by the State, in the person of its organ or its agent acting officially. According to this view, a private operator does not enter the scope of Article 8. The same conclusion cannot be drawn if one follows the position of van Dijk and van Hoof. For those who base their opinion on case law: "the second paragraph of Article 8 expressly mentions "interference by a public authority". It might be inferred from this that the whole article refers only to acts by the authorities. However, the interpretation equally appears tenable that the first paragraph generally prohibits interference with privacy and the second paragraph permits such interference on particular grounds and exclusively by the public authorities. (...) The article could be invoked before the national courts against a private individual in those system in which the Convention has internal effect. Moreover, article 8 then would imply the obligation for the contracting States to assure respect for privacy by individuals to the best of their ability via the legislature, the administration, and the courts."[55]

In our opinion, it is this last interpretation that should be followed.

Article 8 lays down three conditions for an interference to be considered as legitimate:

First, the interference must be made in accordance with the law. It is commonly believed that the term "law" must be interpreted broadly and as covering not only written law but also unwritten law.[56] The law must, however, be equally accessible and foreseeable. This means that the law must be easily accessible, often through published sources like Court decisions, text books and other publications.[57] The foreseeability requirement implies that: "a norm cannot be regarded as 'law' unless it is formulated with sufficient precision to enable the citizen to regulate his conduct: he must be able — if need be with appropriate advice — to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail."[58] In the case brought before the CNIL, there was no law that could justify the experiment of the *SAPR* at the exception of Article 7 c of Directive 93/89/CEE of 25 October 1993[59] which imposes upon Member States a duty to collect the payment at the toll in a way that best avoids traffic congestion. Such an article is, however, too broad to enable citizens to regulate their conduct. Therefore, the decision of the CNIL seems easily understandable and justified: without law, there should be no interference to privacy whatever the quality (private or public) of the party and, in consequence no flash of the registration plate for ensuring a good perception at the tolling.

The two other conditions[60] mentioned in Article 8, for the purpose of legitimating an interference, do not need to be further analysed regarding the CNIL decision. They are, however, helpful for an understanding of Article 6 of the EC Directive on Data Protection. The second condition concerns the purpose for the interference in the privacy. The interference should be necessary for the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of rights and freedoms of others. There is again a broad margin of interpretation for those criteria. The last condition requires that the measure be necessary in a democratic society. As to the question of whether a restriction to privacy is necessary, "the national authorities are allowed a very broad "margin of appreciation".[61] The Convention does not seem particularly helpful since the criteria used are really wide as well. It seems finally that the Court in judging a case will determine whether the interference at issue is proportionate to the legitimate aim pursued and whether the reasons adduced to justify it are "relevant and sufficient".[62]

With regard to the choice between the different projects, the criteria of proportionality requires that as between the measures foreseen for accomplishing the purpose of having an automatic tolling system for security reasons and for avoiding traffic congestion, the least harmful challenge to privacy must be chosen. Therefore, one has to ask the question which of the projects best satisfies this principle, assuming that one is not confronted with the problem of obtaining the data subject's consent. A quick overview suggests the following:

The best level of compliance with the privacy and data protection issues can be found in projects that need less participants for forming the association which comprise the controller. It seems indeed somewhat dangerous to multiply the number of persons or entities that may have access to data related to the individual right of mobility.[63] Therefore, it suggests a preference for projects such as the Mans project (deferred payment) or experimented upon by the Adept II project which assumes that the smart card will not be reloaded. With regard to AAI technology, one can ask whether the string of information necessarily has to identify an account number. It would seem that a simple piece of information communicated to a bank would perhaps best comply with the proportionality principle. Finally, it might be suggested that the road user be given a choice to maintain alternative payment facilities so that he can select whatever form he wants (e.g. a more anonymous method of payment. However, by accepting that he will not receive a proof of payment[64] or deferred payment which is less respectful of privacy albeit with a better possibility of control...).[65]

Such projects should in any way be organized by a law that answers the following criterium: the purpose of the processing imposed by law should be pertinent, sufficient and accompanied by warranties. Moreover, the law should state expressly that the purpose of the processing must at any time comply with the purpose it describes and may not be changed.

### 3. Collect data that must be adequate, relevant and not excessive

According to Article 6c of the Directive, the personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed. This Article refers to the concept of data compliance. A legitimate and specified purpose does not in itself authorize use of any data. For each purpose specified, a sufficient connection must be established beyond doubt between the purpose and the data collected. Any irrelevant data must be discarded.[66] Such an Article does not in itself create a problem. Simply, one can remark that the operator should only be authorized to collect data in line with the purpose of allowing a good recovery of the road fees at the tolling place and no more. Therefore, the following potential secondary use of data must be strictly forbidden:

- data regarding the speed of the drivers;
- the drivers' habit of driving and the infraction regarding the Highway code;
- where you live and when you are coming home;
- at what time you are going to work or go shopping;
- your place of worship and how often you go there;
- where your children go to school;
- where your friends live.

An exception to the interdiction of secondary use could be foreseen for data used for statistical purposes.[67] Such use of the data should not necessarily be strictly forbidden provided that the subject cannot be identified. In other words, the data should be rendered entirely anonymous.

Some public authorities may, however, be tempted to use personal data for the purpose of repressing fraud. In that case the question whether or not, an exception to Article 6, which should be foreseen in favour of prosecutors and jurisdictional authorities may come to light.[68] Article 14 of the Telecommunication Directive[69] allows such derogation for the purpose of preventing and detecting criminal offences. With regard to the adoption of an automatic tolling system,

some individuals may wish to apply for such an exception. Would it be advisable? It is not up to us to decide. Let us just remark that it seems dangerous. As the CNIL did, one would like to insist on the limited rule of the operators and specify that they are not in charge of any policy development. Therefore, they should not participate, even indirectly, towards other activities regarding so many important data. In addition, this could lead to the development of a super-State that could at any moment, define an interest justifying the right to know all of our movements. If, in spite of this, such derogation was adopted, we think that it would at least not lead to a change in the conservation principle laid down in the following section. Indeed, if that was the case, it would become impossible to fix a limited period of conservation of the data for the operators.

### 4. Conserve data during a limited period

Data must also not be kept longer than is necessary for the purpose for which the data were collected or for which they are further processed.[70] In specie, the purpose of most data collected (flash of the registration plate, time of the crossing, and kilometres travelled) is to make sure that a payment has been made and to keep a proof of the payment in case of dispute.

The duration of conservation may depend on the project chosen. It seems *a priori* easier for projects like those using deferred payment or those using smart cards (non-reloaded) to determine the period during which the data may be conserved. According to the conservation principle, for deferred payment, the data should only be conserved for a period of, for example, 10 days following the reception of the bill except in case of dispute.

Regarding deferred payment, the driver may be interested in receiving itemized bills in order to verify the correctness of the fees charged by the operators in respect of the kilometres travelled. However, as it has been pointed out in the Directive concerning the processing of personal data and the protection of privacy in the telecommunication sector,[71] it may jeopardise the privacy. Therefore, it may be recommended to Member States, as the telecommunication Directive did, to encourage alternative payment facilities.

### 5. Fair and lawful processing

Article 6 1 (a) requires that personal data must be processed fairly and lawfully. This means that the processing must be made in accordance with the legislation and in conformity to the transparency principle. The data subject must therefore be clearly aware of the uses of data relating to him, either when the data is collected, recorded or first disclosed.

According to Article 22 and following, the violation of such articles is sanctioned by the provisions of national law.

### 6. No automated decision

Article 15 of the Directive provides that individuals have a right not to be subject to a decision which produces legal effects for them or significantly affects them and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to them, such as performance at work, credit worthiness, reliability, conduct or anything else.

This negative obligation would seem to require operators, controlling a database of bad payers, not to preclude a driver from using the autoRoad even if that individual never pays.

However, for the efficient operation of the automatic system, it would seem advisable for Member States to lay down legal measures (on the basis of Article 15.2b) authorizing operators to forbid a driver from using a motorway if the computer system has identified that person as a recurrent non- payer. The data subject's legitimate interest could be safeguarded by, for example, a warning sent by registered post, prior to the decision threatening prohibition of the use of the motorway. The data subject should have at least a 15 days to respond before the notice comes into effect.

## THE DATA SUBJECTS' RIGHTS

According to article 10 of the Directive, the data subject has the right to obtain a series of information when data relating to himself are collected. Moreover, Article 12 recognizes a right of access (designed to promote the accuracy of the data while ensuring that it is kept up to date) and a right of rectification. Those rights seem precious particularly regarding the fact that some data collected may be wrong since the association between the driver and the owner of the registration plate are not always the same. However in practice they appear quite theoretical. The difficulty in giving such information to the user has already been explained. There is also the problem of giving the data subject an effective right of access since the data are collected in all European countries. The temptation will be strong to have recourse to the exception provided by Article 13. According to this Article, Member States may adopt *legislative* measures to restrict the scope of such rights when such a measure constitutes a necessary safeguard, e.g. for the purposes of national security, defence, public security, the prosecution of criminal offence, important economic and financial interests, official authority or protection of data subjects. Such exception reminds one of the exception confirmed in Article 8 of the Convention. In the present case any legislative action would probably be based on the necessity to safeguard the public security of Member States.

## CONCLUSION

The aim of this article has been to analyse in relation to some EU projects, how an automatic tolling system might be used in conformity with the Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data and whether or not such Directive offers sufficient protection for the individual.

It started with the submission that each automatic tolling system will have to answer to common technical features. Among those features, the use of the flash of the registration plate appears particularly important not only in relation to securing payment and pursuing fraud but also in confirming to the driver that the correct sum has been paid.

The analysis leads to the conclusion that legislation common to all European Member States is desirable. In assuming

responsibility for proposing recommendations as to the content of the Directive that could be adopted, the following necessities come to mind: (i) the possibility of different payment methods; (ii) the need to determine by what conditions a flash of the registration plate might be authorized by fixing a clear and sufficient purpose for processing accompanied by warranties; (iii) the establishment of minimum of requirements for standards of security regarding the quality and appropriate use of the instrument used to collect the data and to stock it; (iv) identifying the person jointly to be considered as Controller and the purpose of the data collection. The Directive should also apply to legal entities and offer protection to the employees; (v) all secondary use of the data and all modification of such purpose should be clearly forbidden; (vi) the period of the data conservation should also be fixed; (vii) a general right of access and use of the data by public authorities (mainly prosecutors) should be forbidden; (viii) an automated decision should be permitted but must be accompanied by safeguard measures. It seems that this is the price to be paid to protect the privacy of individuals and avoid the birth of *Big Brother*.

**Jean-François Lerouge**, assistant and Researcher,
Research Centre for Computers and Law, Facultés Universitaires, Notre-Dame de la Paix de Namur, Belgium

## FOOTNOTES

[1]This article is written in the context of a contract with the DG VII and the CRID. It represents the author's opinion and is his sole responsibility. The author would like to thank S. Louveaux and Y. Poullet for their wise advice regarding this paper.

[2]Newspaper *Le soir*, 15 April 1999, p. 5. Regarding this, in Belgium, a system of road pricing has not been recommended for the time being. However, the federal state has been encouraged, following the development of an interoperable system at an international level, to follow carefully technological development in such matters and the experience of other countries (see Report of the University of Liege, UFSIA and CIRIEC, "Etude préparatoire à la définition d'un plan fédéral de mobilité durable", note d'orientations, November 1998, p. 27).

[3]The idea often cited is to establish a system of "grilles tarifaires". See Communication de la Commission: "Interopérabilité des systèmes de péages en Europe", Com (1998) 795, final.

[4]The company Thomson: <http://www.tcc.thomson-csf.com> in May 1996 concluded an agreement with operators in Italy regarding an automatic tolling system without barrier. The system works with a flash of the registration plate. In France such a system has not been accepted by the Commission for privacy. For more information see hereafter. In the UK, the Driver and Vehicle Licensing Agency (DVLA) is working on automated number plate reading technology among others to be used as one component of motorway tolling. Regarding privacy, the Department of Transport stipulates without going further that any such use would, of course, be covered by the Data Protection Act 1998. For further details, see Department of the Environment, Transport and the Regions, *A policy for using new telematic technologies for road transport, consultation document*, available at the following address: <http://www.roads.detr.gov.uk/roadnetwork/ditm/doc4c.htm>.

[5]For a brief outline of those projects, see: <http://www.trentel.org/transport/research/11.html>.

[6]See Communication de la Commission, *op.cit.*, p. 14.

[7]Directive 95/46/C.E. of the European Parliament and the Council of October 1995 *on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, O.J., n°L281/31, of 23 November 1995.

[8]See, for example, the system Digital Cash invented by David Chaum. Such a system is said to be an inherently anonymous toll payment. This should, however, be demonstrated with regard to the system used for repressing fraud. Moreover, it seems that such a system raises legal questions regarding money laundering. For more details see P. Agre, "Looking Down the Road", *The CPSR News*, Fall 1995, p. 15; T. Wright, "Coup d'oeil sur la route: systèmes intelligents de transport et vie privée", Commissaire à l'information et à la protection de la vie privée/Ontario.

[9]An example may be found in Orlando, Florida. The E-Pass system in Orlando issues each customer a monthly statement that includes the customer's name and address, together with a complete list of toll payments for the month. Each entry on this statement lists the precise time and location of the toll payment, including which lane the driver was in. For more details, see P. Agre, "Looking Down the Road", *The CPSR Newsletter*, Fall 1995, p. 16.

[10]In the Netherlands, the Minister van Verkeer takes into consideration the possibility of installing an automatic tolling system which will work by satellite. The user will be billed by the distance in kilometers covered. The system could be implemented in 2001. Source: *De morgen*, 30 March 1999.

[11]Such dual objective is well illustrated by article 1. For a comment of the directive, article by article, see Cullen International, C.R.I.D., *A Business Guide to Changes in European Data Protection Legislation*, Kluwer Law International, 1999, XXVII, 321 p.

[12]For an analysis of the regulatory systems or lack of them in the Netherlands, United Kingdom and Germany with regard to the EC Directive, see European Commission, *Existing case-law on compliance with data protection laws and principles in the Member States of the European Union*, edited by Douwe Korff, 1998, 65 p.

[13]Y. Poullet, "Flexibility in the Directive", in Cullen International, C.R.I.D, "Directive 95/46/EC, The Informed View, A Business Guide to Changes in European Data Protection Legislation part 4". "The Member States dispose of a margin of manoeuvrability which, in the context of putting the directive into practice, could be made use of by their economic and social partners. This would enable them to adjust precisely to the general conditions for data processing permission contained in their national legislations and by so doing strengthen current protective provisions. Disparities might therefore appear in the carrying out of the directive, assuming these are within this margin and in conformity with community law".

[14]See M.-H. Boulanger, C. de Terwangne, Th. Léonard, S. Louveaux, D. Moreau and Y. Poullet, "La protection des données à caractère personnel en droit communautaire", *J.T.D.E*, 1997, p. 124.

[15]We will see, however, that such agreement is not easy to obtain with regard notably the free consent of the data subject.

[16]Cullen International, C.R.I.D, *op.cit.*, p. 27; M.-H. Boulanger, C. de

Terwangne, Th. Léonard, S. Louveaux, D. Moreau and Y. Poullet, *op.cit.*, p. 124; European Court of Human Right, *Huvig Case*, 24 April 1990, série A, n°176-B, p. 41 §8 and p. 52 §25.

[17]Cullen International, C.R.I.D, *op.cit.*, p. 26 , M.-H. Boulanger, C. de Terwangne, Th. Léonard, S. Louveaux, D. Moreau and Y. Poullet, *op.cit.*, p. 124.

[18]M.-H. Boulanger, C. de Terwangne, Th. Léonard, S. Louveaux, D. Moreau and Y. Poullet, *op.cit.*, p. 124.

[19]However, let us just remind ourselves that the legal person would have to inform their employees that, by using a motorway, it may be possible for the company to know exactly where they went, on what time…

[20]See for example: l'exposé des motifs of the Belgium law of 11 December 1998. It clearly rejects such interpretation. The Italian and Austrian law includes legal persons in scope of protection offered by national data protection law, see article 1.1. of the Italian Law n°675 of the 31 December 1996 and Sec.3 (2) of the Austrian Datenschutzgesetz BGB1 1978/565. Besides, we can wonder if this distinction between legal entity and physical person is still justified. As a reminder, Article 2 of the Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector (*O.J.*, L 024, 30 January 1998) does not make such a distinction anymore.

[21]If the Directive does not apply, the Human Rights Convention of 4 November 1950 still applies.

[22]See the study of the proton cart L. Petit and A. De Vylder, "Monnaie électronique et libertés individuelles", *Ubiquité*, 29 to 45. The authors insist on the importance of the data collected at the moment of the loading and the payment. Since there is a link between the number of the card and the number of the account holder, it is possible for the bank to identify the issuer of the card when he pays the trader.

[23]Communication de la Commission, *op.cit.*, p.12.

[24]Recommendation n°R (91) 10 of the Comite of Ministers available at the following address: <http://www.coe.fr/DataProtection/rec/r(91)10f.htm>.

[25]See also the Green Paper on Public sector information in the information society, Com (1998) 585.

[26]See hereafter, Section C.

[27]According to Article 2e, a processor is a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller. In such a case, it will be the liability of the controller to watch over the security of the processing.

[28]We will hereafter demonstrate that an automatic road tolling may be difficult to organize other than by a common law in each European country.

[29]Article 2 (h) of the Directive.

[30]Example in case of sensible data.

[31]M.-H. Boulanger, C. de Terwangne, Th. Léonard, S. Louveaux, D. Moreau and Y. Poullet, *op.cit.*, p. 126.

[32]In such a case, we can also argue that the citizen's right of mobility is affected.

[33]M.-H. Boulanger, C. de Terwangne, Th. Léonard, S. Louveaux, D. Moreau and Y. Poullet, *op.cit.*, p. 126. For a comment regarding the finalities.

[34]Cullen International, C.R.I.D, *op.cit.*, p. 35.

[35]The conclusion of a specific contract with operators may be difficult since different operators using the automatic tolling system may share the territory.

[36]In order to comply with the wording of Article 10.

[37]Case C-153/93, June 1994, 9 (Delta Schiffahrts-und Speditionsgesellschaft), *Rec.*, 1995, I-2519 (confirmed by case n°C-38/97, 1 October, 1998, where the Court concluded that the concepts of general interest and public interest have the same meaning). In the case at hand the problem examined by the Court was related to a legislation of a Member State which provides for road-haulage tariffs to be approved and brought into force by the State on the basis of proposals of a central committee.

[38]See, for example, the Belgian declaration of Constitution revision. The declaration forsees the insertion in Article 23 of the Constitution of a citizen's right to a minimum service in the field of mobility.

[39]See Recitals of the Council Resolution of 17 June 1997 regarding the use of telematic in road transport, *O.J.*, 1997, n° C 194/5. See also Article 7 c of Directive 93/89/CEE of 25 October 1993 (*O.J.*, 1993, n° L 279) which imposes to Member States to control the collection of the payment at the toll in a way that is the best for avoiding traffic congestion.

[40]When the running of service is fully dealt with by private operators, one can understand why they might decide together to establish an automatic tolling system without contracting with the public authorities.

[41]Indeed, the question is how to comply with this article, if the data subject has no other choice than to accept the processing?

[42]See hereafter Section 2.

[43]Confirmed by Article 14.

[44]Article 6 (1) (b) of the Directive.

[45]Article 6 (1) (c) of the Directive.

[46]M.-H. Boulanger, C. de Terwangne and Th. Léonard, "La loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard du traitement de données à caractère personnel", *J.T.*, 1993, p. 377.

[47]Such convention came into force on 1 October 1985 and currently binds the government of the following countries: Austria, France, Germany, Italy, Luxembourg, the Netherlands, Spain, and the United Kingdom. The purpose of the Convention is to secure the individual right to privacy with regard to automatic processing of personal data relating to him. The Convention is still in force and may be used in the countries signatories as a source of law.

[48]Convention of 4 November 1950.

[49]Case *Dudgeon*, 30 January 1981, Serie A n°45, p.28; case *Sunday Times*, 27 October 1978, série A, n°30, p.38, Case *Olsson*, 24 March 1988, série A, n°130, p. 32.

[50]CNIL, 17th Report of activity, 1996, p. 100 and f. Following a recent contact with the CNIL, they informed us that no other cases have been bought to the Commission.

[51]Eurotunnel and the distance reading of registration plates, see CNIL, 16[e] rapport d'activités, 1995, pp. 233–235.

[52]The latest remark brings us to remind the reader that the Directive does not apply to the processing of personal data in the course of criminal investigations. However, Article 8 of the Convention will still have to be taken into consideration.

[53]L-E Pettiti (sous la direction de), *La Convention européenne des droits de l'homme, commentaire article par article*, ed. Economica, Paris, 1995, p. 329.

[54]A.c. France, 23 November 1993, A n°277-B, §36.

[55]P. van Dijk and G.J.H. van Hoof, *Theory and Practice of the European Convention on Human Rights*, Kluwer, Second Edition, 1990, p. 372.

[56]P. van Dijk and G.J.H. van Hoof, *op.cit.*, p. 579; L-E Pettiti, *op.cit.*, p. 334 and f.

[57]See Judgment of 26 April 1979, *Sunday Times*, A.30 (1979); also

Judgment of 25 March 1983, *Silver*, A.61 (1983), pp. 33–38.

[58]The *Silver* case, *ibidem*, p. 33.

[59]*O.J.*, 1993, n° L 279. For reminder, Directives have, following Articles 5 and 189, a direct effect. For more details, see J. Verhoeven, *Droit de la Communauté Européenne*, Larcier, 1996, p. 267.

[60]Following the classification made by Pettiti, *op.cit*, p.333 and f.

[61]P. van Dijk and G.J.H. van Hoof, *op.cit.*, p. 585; L-E Pettiti, *op.cit.*, p. 337 and f.

[62]*Lingens* case, Judgement of 25 March 1983, A.61 (1983), pp. 37–38.

[63]We personally regret that such fundamental data are not classified by the Directive inside the category of *special categories of processing for which special protection is offered.*

[64]For a consumer protection point of view, it seems to us, however, that the operator should supply the user with a way (e.g. by a card reader) to find information relating to the transactions effected by means of its smart card.

[65]For example, in the same way as Article 7 of the Telecommunication Directive which gives the subscribers the right to receive non-itemized bills.

[66]Cullen International, C.R.I.D, *op.cit.*, p. 43.

[67]Regarding the processing for statistical purposes, see the Recommendation No.R (97) 18 and Explanatory Memorandum of the committee of ministers to member states concerning the protection of personal data collected and processed for statistical purposes, available at the following address: <http://www.coe.fr/DataProtection/rec/r(97)18e.htm>.

[68]For a description of the rules that should be applied regarding the communication of personal data by a public organizations to third parties, see Recommendation n°R (91) 10 of the Comite of Ministers available at the following address: <http://www.coe.fr/DataProtection/rec/r(91)10f.htm>.

[69]Directive 97/66/EC of the European Parliament and of the Council, *OJ*, L24, 30 January 1998. See also the Recommendation 1/99 adopted on 23 February 1999 by the data protection party on Invisible and Automatic Processing of Personal Data on the Internet Performed by Software and Hardware, available at the following address: <http://europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/index.htm>.

[70]Article 6. (1) (e) of the Directive.

[71]Recital 18 and Article 7 of the directive 97/66/EC, *op.cit.*

## Book Review

### Intellectual Property

Practical Intellectual Property, compiled and edited by Denton Hall (Solicitors), 1992, plus 13 supplements to April 1999, loose-leaf ringbinder, Gee Publishing Ltd, ISBN 0 85258 909 3

Gee Publishing has been publishing information for business and professionals since 1874. In 1980 the company became part of the Thompson Corporation, and since then has rapidly expanded its activities. This includes loose-leaf subscription information services, but also magazines, periodicals, information on disk, CD-ROMs and over the Internet. This book is intended to be used as a manual or guide book rather than to be read from start to finish. It aims to provide a working guide to users of intellectual property in the UK. Its authors suggest that the book is in response to growing awareness of intellectual property and its significance in industry. The work is divided into four parts. Following an introductory section, Part 2 deals with protection and exploitation of individual rights (Chapters 2–11). This consists of a guide to intellectual property in general terms describing the individual's rights in separate chapters. The third part — enforcement of rights (Chapters 12–14) explains how the rights described in Part 2 can be enforced. It discusses relevant legal and procedural requirements as well as practical guidance on how to run litigation at management level. The final part, Section 4 — application of rights to specific industries (Chapters 15–20) — examines how intellectual property law is relevant to particular industries. These include the computer industry; retail and distributive trades; service providers; manufacturing industries; the biotechnology industry, and research and development. The text is updated twice yearly with a supplement.

Available from Gee Publishing Ltd, 100 Avenue Road, Swiss Cottage, London, NW3 3PG, UK; Tel: +44 171 3937400 or Fax: +44 171 3937463; Internet: <www.gee.co.uk>.