Legal conditions for implementing EDRs in public fleets of vehicles

Michèle Guilbot, Thierry Serre, Claire Naude, Vincent Ledoux

ITS- EU-SP0293

Legal conditions for implementing EDRs in public fleets of vehicles

Michèle Guilbot[1], Thierry Serre[1*], Claire Naude[1], Vincent Ledoux[2]
1. IFSTTAR Laboratory of Accident Mechanism Analysis, 304 chemin de la Croix Blanche, 13300 Salon de Provence, France, +33490568653, thierry.serre@ifsttar.fr
2. CEREMA Technical Division for Territorial Development and Urban Planning, 2 rue Antoine Charial, 69426 Lyon, France, +33472745956, vincent.ledoux@cerema.fr

Abstract
This article describes how the legal conditions for collecting and processing data collected with event data recorders in vehicles (EDR) must be taken into consideration in a context of operationally-oriented road safety research. Because these data can allow to identify drivers of vehicles, directly or indirectly,the technical and organizational conditions must comply with European and country legislation on the protection of personal data and privacy. Potential drivers must volunteer to have the recorder on board and for data collection. Consent must be freely given, be informed and specific. The EDR must not affect vehicle safety. Specific conditions apply when vehicles are service vehicles potentially driven by different agents on duty.All these legal requirements have been applied for an experiment conducted in France. They can be transferred to other European countries because they are based on EU rules and principles derived from the European Convention on Human Rights.

Keyword(s):
data logger, legal issues, public fleets, personal data protection, privacy

1. Introduction

Road event data recorders (EDRs) are increasingly used to conduct studies and research in the field of road safety and traffic or to allow services to be delivered to users, such as real-time services for traffic information or deferred services such as adjustment to insurance premiums. In the field of research, they are the main tool for performing studies like "Naturalistic Driving" type [1, 2, 3]. But because such a system can record data that can be used to identify drivers and learn their travelling and driving habits, it is important to be familiar with the technical and legal requirements for installing them in vehicles and implementing collection in full compliance with the laws. The issue of the confidentiality of personal data is one of the main concerns to be considered when the data is collected with EDRs [4].
EDRs may be instrumented on private vehicles but also in national or local private company or public fleets, i.e., in cases where vehicles are not necessarily assigned to a single person and can be driven by different people in a professional context. More specific terms of protection must then be respected due to the hierarchical relationship between the drivers and the vehicle owner (usually the employer).
In 2010, the French Government (DSCR[1]) decided to support a new research programme based on the analysis of traffic incident data. This project called S_VRAI (Saving Lives by Road Incident Analysis Feedback) brings together IFSTTAR and Cerema (two public research institutions) with road infrastructure managers. One of the project's objectives was to implement EDR in public vehicle fleets to analyse incidents in three geographical areas for a collection period of one year (August 2012 to July 2013) [5].
The first step was to ensure that the experiment was legal, especially the respect of drivers' right to protection of their personal data and privacy. Although these conditions were applied for a French project, they are transferable to most European (and possibly international) projects because they are based on the requirements of respect for human rights and on EU rules.
This action was in itself one of the goals of the research. The article will therefore be mainly focused on the issue of the protection of the personal data and privacy of drivers of vehicles equipped for experimentation and the technical and organizational procedures enabling these rights to be guaranteed (section 3). Before

[1]Interministerial delegation for road safety

this, we will describe the project in general terms and some of the legal requirements related to other considerations (section 2).

2. The S_VRAI project

This project was based on an EDR called EMMA (Embedded data logger for accident mechanisms). It was designed by IFSTTAR's MA laboratory with the help of Kerlink[2], a small company specializing in "Machine to Machine" [6].
The main ideas followed in order to design this EDR were:

- facilitating the work of staff in charge of vehicle fleets to implement them in vehicles and for data collection, with automatic transfer via a secure GSM connection;
- complying with the regulations and recommendations of the CNIL 3 by limiting periods of data acquisition to situations of interest from the standpoint of research. Only incidents and collection in specific areas defined by the team as areas of interest in terms of road risk were considered [6].

Within the meaning of the S_VRAI project an incident can be defined as an event occurring during an action that may disrupt a normal driving situation.
From a conceptual point of view, the incident will correspond to a break in the user's normal driving situation that marks a shift to a degraded situation (incident). Without an appropriate emergency manoeuvre this situation could result in a collision or a loss of control which could have material or personal injury consequences (accident).
From an operational point of view, an incident is a driving situation where a user is close to an accident situation. For example, when the driver performs an avoidance manoeuvre or brakes heavily, or when, in order to stay in lane in a bend, undergoes lateral acceleration close to the safety threshold.
To characterize the driving situation, the EMMA continuously acquires:

- analogue data from sensors directly integrated into the EDR (accelerometers and gyros),
- data from a GPS (trajectory and speed),
- available data passing through the BusCan, the availability of which depends on the vehicle model.

The data are first analysed using real-time processing performed by the on-board software to detect potential interest situations (events). Processing is based on the following principles: when acceleration and jerk signals exceed a threshold at the same time, an event is triggered [4, 5]. Data are acquired 30 seconds before and 15 seconds after triggering at a frequency of 100 Hz and stored in the system that automatically generates an electronic report of the event (GPS positions, values of dynamic parameters and a simplified speed profile). This report is then automatically sent to IFSTTAR servers for examination. If the event is considered to be of interest, all the data, at a frequency of 100 Hz is downloaded for detailed analysis.
Fifty EMMAs were installed on board the fleets of four public agencies (2 road managers and 2 research institutions).
These fleets were located in northern France (Normandy-Centre region) in the centre (Auvergne region) and in the south (around Salon de Provence). More than 200 people likely to drive these vehicles agreed to participate in the experiment. Among these, over 150 also agreed to provide personal information: gender, year of birth and the date they obtained their driving license. This information was associated with an individual code obtained using hashing algorithms and stored in a personal magnetic card. These cards were sent to volunteers who could decide at the beginning of each journey whether or not to send their code to the EDR using an RFID reader installed in the vehicle. For other drivers or if the card was not red only data on driving and vehicle dynamics was collected. In addition, to respect the fact that participation was voluntary, for the reasons explained below, the drivers always had the option of disabling or not enabling the acquisition system.
In terms of safety and security, the technical conditions to implement EDRs in vehicles are as follows:

- The EDR must meet EU standards in terms of electromagnetic compatibility (EMC) and radio and telecommunications terminal equipment (R & TTE).
- The procedure for installing EDRs does not change vehicle compliance with respect to safety and respect for homologation and approval procedures.

[2] http://www.kerlink.fr
[3] *Commission Nationale de l'Informatique et des Libertés* - National Commission for Computing and Liberties, the French administrative authority responsible for supervising the protection of individuals' personal data.

Verifying these conditions allows compliance with regulations on vehicles and provides a guarantee against liability waivers by the insurer in the event of an accident.
These requirements were met in the S_VRAI project by conducting tests to ensure that the EMMA boxes were compliant with the regulatory requirements in force for EMC and RTTE. This made it possible to obtain from the Ministry of Transport a one-off exemption for vehicles equipped with EMMA, and put into service without any further formality.
Over and above "EDR technique" compliance, one of the main challenges of the project involved implementing measures to protect the personal data that these EDRs can collect.

3. EDRs and the protection of drivers' personal data

The collection and processing of personal data raises ethical issues which the law may be the bearer of to protect the rights of those concerned. It is therefore necessary to determine the data that can be directly or indirectly identifying in the specified context. This then makes it possible to take the best protection measures in the event of it not being possible to perform irreversible anonymization, at least during the period of collection and analysis. During this period, some of these data are necessary for the management of the fleets of vehicles and boxes, as well as for the study itself. It is also necessary to determine the legal basis for collecting and processing data. Finally, in the light of the principles laid down by national or European rules, measures should then ensure the confidentiality and security of these data. These technical or organizational measures are the backbone of the implementation conditions for processing the data collected by an EDR.

3.1 The personal nature of data collected by the EDR

The regulatory requirements applicable in France are borne not only by domestic law (law 78-17 modified on 6 January 1978, compliance with which is controlled by the CNIL), but also by European laws. The United States are starting to develop legislation in the same direction.
The European Union (28 Member States) included the protection of personal data in EU law in 1995 (Directive 95/46/EC of October 24, 1995). Since 2012, a reform of the directive has been undertaken which has been replaced recently by a regulation directly applicable in domestic law[4]. This protection is equivalent to a fundamental right since the coming into force of the Lisbon Treaty in 2009 which recognizes the rights, freedoms and principles of the European Charter of Fundamental Rights of 2000 (European Union treaty, Art.6.1; Charter, art 7, privacy; Art.8, personal data). For its part, the Europe of Human Rights (47 Member States) long ago sanctioned this protection (European Convention on Human Rights, 1950, Art. 8, privacy) and Convention of January 28, 1981 called the "convention n° 108" (personal data).
In the US, most recent motor vehicles are equipped with EDR. The Electronic Code of Federal Regulations specifies the rules concerning them (§563.6 et seq.). Some States have developed protection of drivers' rights. 17 states adopted rules for EDRs and the protection of privacy. Some have made provision for the fact that collections can only be made with the consent of the vehicle owner or driver, subject to exceptions. In 2015, federal law placed limits on data recovery via EDRs and issued a reminder that these data belong to the owner or hirer of the vehicle[5].
In this way, the desire to protect personal data is not a special feature of France and is compulsory in many countries[6]. The events of recent months have shown the ability of European authorities to shake things up in order to take better account of the rights of people concerned by the processing of personal data, such as invalidating the Safe Harbor principle [8]. Future EU rules act in the same direction and will be applicable in the field of on-board recorders in vehicles as they will more broadly to connected vehicles.

<u>Personal data</u>
Personal data are characterized by the fact that they enable the identification and profiling of a person. In this case, the use of an EDR can be used to characterize his/her driving behaviour and travel habits. It is essential

[4] Regulation adopted the 14th of April 2016 by the to be effective in 2018. Legislative resolution of the European Parliament (05419/1/2016 - C8 - 0140/2016 - 2012/0011 (COD)).
[5] http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-of-data-from-event-data-recorders.aspx.
[6] The mandatory nature is characterized by the ability of the legal and supervisory authorities to impose penalties.

to remember that the notion of personal data is not limited to privacy. The data are personal if other data that might enable the person to be identified are also collected.
Under French law, personal data consists of *"any information relating to an identified person or one who can be identified, directly or indirectly, by reference to one or more features that are specific to him/her. To determine whether a person is identifiable, all the means enabling him/her to be identified which the person in charge of processing or any other person has or may have access to should be considered"*(law 78-17, Art. 2). The 1995 directive refers to "an identification number" and to "specific features" proper to the "physical, physiological, mental, economic, cultural or social identity" of the person. The future European regulation also refers to "location data", an addition that has an impact in the field of mobility and road risk.
The source of the collection and identification matters little: the person concerned, an on-board data recorder, a navigation system, a smartphone connected to the dashboard, the combination of multiple data, etc. In the field of on-board recorders in vehicles, many data allow identification of the driver: the vehicle identification number, the serial number of the EDR, the IP number of an on-board computer, the MAC address of a smartphone, etc. [9, 10]. This identification then makes it possible to characterize his driving activity (for example when did he start braking before a collision or actuated any other control?) or even to try to define a driver behaviour profile (aggressive, etc.) by analysing his accelerations.
Among the data that are useful in the field of road safety research, the most critical are geolocation and data which can characterize an offence, such as speed at a given time in combination with geolocation. Contextualization by means of video is also very valuable, but poses some problems with regard to recognizing people.

Geolocation

Geolocation opens up vast perspectives in the field of road safety and mobility analysis. But it is also used to qualify the place of the object in space at any time regardless of the location technologies used (GPS, WiFi, Bluetooth) and on-board communication devices (sensors installed in a vehicle, navigation systems, smartphones , etc.). In doing so, it informs on where the carrier of the object is located, makes it possible to trace his/her movements and habits (living places, places he/she goes to, etc.). According to the G29[7], smart mobile devices are "*inextricably linked to individuals". "It is usually possible to identify them directly or indirectly"* [11]. In other words, geolocation is an indirect identifier. Researchers have shown that 4 location points were sufficient to allow 95% reidentification of 1.5 million mobile phone users even though none of the data collected was an identifier on its own [12]. Origin-destination points are also sensitive because they identify dwelling places, particularly in relatively isolated areas or in the case of collection with a certain amount of frequency. Cross-referencing them with information from other databases, such as sociodemographic or vehicle registration databases, reinforces their ability to draw the profiles of people identifiable through their travel or driving behaviour.
Location data are protected under the 2002 "privacy and electronic communications" directive which recalls the requirements for protection of personal data laid down by the 1995 directive and the fundamental rights recognized by the EU's Charter of Fundamental Rights. The 2002 directive defines location data as *"any data processed in an electronic communications network or by an electronic communications service, indicating the geographic position of the terminal equipment of a user of a publicly accessible electronic communication"* (Art. 2c)[8].
Limits on the use of location data have been laid down by the authorities protecting personal data, for example when examining the e-Call system (on-board emergency warning system), especially with regard to insurers and motor vehicle manufacturers. As these devices should not allow constant tracking of vehicles, permanent connection is ruled out [9, 13, 14]. The CNIL has validated the e-Call because the alert is triggered only after the collision and its sole purpose is to alert the emergency services (CNIL, deliberation 2010-096). The future European regulation is intended to apply the principles of protection to any information concerning an identified or identifiable person, the location data being in this text considered as an identifier (recital 24, Art. 4). Though any data associated to geolocation will be consider as personal data.

[7] Group for the protection of individuals with regard to the processing of personal data established under Article 29 of the 1995 directive. Its mission is to provide advice and recommendations on data protection. It is composed of the presidents of supervisory authorities of the countries of the European Union (CNIL in France) and representatives of European institutions such as the European Data Protection Supervisor.
[8] European Parliament and the Council, "The processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)," Directive 2002/58/EC, 12 July, 2002.

In the S_VRAI project two geolocation categories were considered:

1) The first concerns the need to have information about the 30 seconds prior to triggering the system and the 15 seconds following it. This information is essential for understanding the incident or accident since it is agreed to decompose the course of the accident sequentially as follows [15]:

- The driving situation, which corresponds to the "normal" situation for the driver during which he is in control of his vehicle.
- The disruption point, which corresponds to an interruption of the driving situation which thereby puts the system in danger.
- The emergency situation, which covers the space-time between the break point and the collision.
- The collision situation that encompasses the nature of the collision and its consequences

As these geo-tagged data are limited to 45 seconds around the incident but have to be fine for a thorough analysis, the GPS position were recorded at a frequency of 1 Hz.

2) The second relates to the needs expressed in order to know the road sections on which the vehicle fleets are driving. They concern the GPS traces of all routes of each vehicle. In accident research, one of the most frequently used indicators is the accident rate. It is calculated for a road section by dividing the number of accidents on this section by the number of kilometres travelled on the same section (the notion of risk exposure). The accident rate is used for the operational needs of network operators such as determining which road sections are at higher risk, evaluating the effectiveness of development work by comparing the accident rates before and after development work, general comparison of groups of road sections, etc.
As GPS traces are only required to characterize traffic on a section on which there is traffic, they do not need to be associated with vehicle drivers, and so their records were "isolated" from driver data. Moreover, as these data may be potentially identifiable, their acquisition frequencies were reduced to 1 pt/min.
In addition, when geolocation is associated with the current speed, knowledge of the speed limit on the section makes it possible to presume that an offence has been committed by the driver. This circumstance is particularly monitored by the CNIL in France.

Offence data

In France, only certain authorities are empowered to be aware of offence data (1978 law, Art. 9). In 2010, the CNIL issued a reminder of its extreme vigilance regarding the collection of offence data, specifically targeting instantaneous speed (deliberation 2010-096, April 8, 2010, which essentially concerned insurers and motor vehicle manufacturers). Considering vehicles with driver assistance systems (e.g. for navigation), it is possible to collect data about the driving speed and about location data. Using them in association is likely to characterize a violation of the regulations on speed limits.
But instantaneous speed and geolocation data are essential for the analysis of road risk. The fact of having continuously available speed measurement with geolocation makes it possible to finely link driving speed and the characteristics of the road infrastructure, thereby allowing further analysis, such as:

- detailed knowledge of the kinematics of driving on improvements designed for road safety.
- knowledge of speeds on secondary networks that are not well known and for which there is a road safety issue from the standpoint of risk.
- knowledge of speeds on urban networks especially those where the deployment of roadside measurement devices is not possible.
- analysis of speeds in connection with the road characteristics (geometry, equipment, service level). This is essential for capitalizing knowledge and drafting recommendation guides for planners and managers.
- analysis of driving speeds (and acceleration) for applications relating to the environment.

In France, the CNIL may grant an authorization for the collection and processing of such data (1978 law, Art. 25-I-3) to public bodies when the need for the collection is legitimized by the intended purpose and the mission assigned to these agencies (public service missions) and when all measures are taken to ensure data confidentiality and security. This was the case for the S_VRAI research project, since the need for having the current speed and geolocation data available was justified as being relevant for their work, and because the research organizations involved in the project are public institutions.
According to the draft European regulation in its current form, the processing of data relating to offences must be authorized by law or placed under control of "public authority" (Art. 9bis).

Context videos

It must be possible to consolidate the quality of the results of a road safety study by viewing the context because it helps answer questions like: what is the event that triggered the system? what was the characteristic of the infrastructure at the time of the incident? in order to perform a diagnosis that will provide a list of relevant actions to be implemented.
The team obtained CNIL permission to film the context as an experiment. To this end additional conditions must be introduced into the protocol: it is essential to blur faces or license plates of vehicles at the source so as not to identify people travelling on public roads. The length of the recording must be linked to the duration of the incident or passing through the area of interest. The continuous acquisition of images on public roads additionally requires authorization from the Interior Ministry.

3.2 The legal bases for implementing a recorder project

While researchers, particularly those from the public sector can access these data for their research mission, this does not exclude the obligation to take appropriate confidentiality and security measures in order to respect the rights of drivers, even though they volunteer to participate in the experiment. Their confidence is based on trustworthiness, legality and transparency of the process, and the legal requirements for collection and processing (1978 law, Art. 6.1 °), confirmed under the future Regulation (Art. 5.1.a) that the research team is firmly committed to respecting.

Legitimate, specified and explicit purposes

Firstly, only data needed to achieve the intended purpose must be collected. These are the principles of necessity and proportionality: data must be adequate, relevant and not excessive (1978 law, Art. 6.3). It is indeed the purpose that determines the choice of data. In the field of scientific research, this corresponds exactly to the rigour required to define the problem, the assumptions and the appropriate methodologies.
The purposes have to be legitimate, specified and explicit.
Legitimacy of purpose based on an identifiable legal basis (1978 law, Art.7; Directive 95/46/EC, Art. 7). In the case of research based on data collected by an EDR, consent will be the legal basis used. The public status and the public service mission with which the partners involved are invested, especially the processing data controller, consolidate the legitimacy of collection and processing. In the case of research, it is true that it is possible not to obtain consent, for example when obtaining it would require disproportionate efforts. But this was not the case here, since the drivers were specifically asked to take part in the experiment.
The explicit nature of the purposes is here to be found in the statement of the research problem and the topics defined: in our case identifying areas for progress in understanding and preventing road risk.
They are explicit because they have been clearly and precisely defined and outlined in the research project and in the briefing notes prepared for people likely to be driving the equipped vehicles.

Free, informed and specific consent

The voluntary nature of drivers' participation is a non-negotiable imperative if collection and processing are not backed by one of the other bases provided for by legal provisions (1978 law, Art. 7;. directive 95/46, Art. 7; future European Regulations, Art. 6).
Consent must therefore be granted "knowingly." It is characterized by *"any manifestation of specific and informed free will, by which the person concerned accepts that the data concerning him/her is to be processed"* (directive 95/46 / EC, Art.2.h).
Three factors characterize it. It must be free, informed and specific. According to the future European regulation, it must also be unambiguous (Art. 4.8) and the processing data controller must be able to demonstrate that consent has really been given (Art. 7). These requirements meet the principle of transparency embodied by an obligation to inform about the purpose of the collection and processing methods (what is it exactly that drivers agree to when clicking an "I accept" icon?).
Free consent: consent is deemed valid if it is independent of any constraint. It must be obtained without pressure and without incentives, particularly where the collection takes place in a professional environment and when a hierarchical relationship may affect consent. Independence is manifested primarily by the option of not consenting [16].
This implies two consequences which were respected for the S_VRAI project:

- default disabling of vehicles that could be driven by different drivers to ensure that non-volunteer drivers ran no risk of having their data recorded;

- reversibility of consent for volunteer drivers without having to justify why, including those driving fleet vehicles (service vehicles) when collection and processing are not necessary for carrying out the professional activity. Withdrawal of participation mighty concerns a particular route (the system is temporary disabled) or be definitive.

Enlightened or informed and specific consent: These conditions require fulfilment of a duty of information on the part of the processing data controller on the use of data (objectives, methods), their future, their recipients: who has access to what and to do what with? The information must be complete, accurate and accessible.

All potential drivers of the equipped vehicle were informed (by written information and/or an oral presentation of the project) about the experiment. Furthermore, since the vehicles equipped were service vehicles being driven for professional reasons, the opinion of staff representatives was collected following an information meeting. Considering that consent must be truly enlightened, drivers were also informed that the recorded data might be required by the judicial authorities, notably if accidents occur.

All the information measures taken made it possible to obtain consent given "knowingly" collected on forms that gave a reminder of the general principles of the project and the commitments of all parties. Collection of written consent makes it possible to attest to its truth and to oblige the person to read the main methods of implementing the experiment.

Prospects for extending aims favourable to research

Consent relates to the purpose and the recipients of the data, which in principle means no re-using of data without previously granted consent from the person concerned by the data, unless authorized or if there is a legal or regulatory obligation.

It may be admitted that it is impossible to obtain consent if there is no other way to achieve the purpose. In this case, a fair balance between the legitimate interests of the processing data controller and the fundamental rights of the person concerned must be struck (see 1978 law, Art. 7 5° and [16]). This possibility is enhanced in the future European regulation for purposes not inconsistent with the initial purposes. Though, the objectives related to research or production of statistics will be presumed to be compatible with the initial purposes, although any identifiable person still has the right to object to the collection.

Specifically, in these circumstances, the right of opposition by the persons concerned will sometimes be difficult to implement. For this reason, in order to allow personal data to be reused in trustworthy conditions, and while it is physically impossible to get back to the person concerned to seek his/her consent, some ideas are suggested. For example setting up a creative Commons type license for the reuse of personal data, inspired by licenses developed in the field of intellectual property rights (Privacy Commons movement). Privacy and security measures will obviously have to be taken.

3.3 Privacy and security

As we have seen above, the fact that the person concerned by the data may possibly be identified requires supporting measures to be implemented to collect and process this data. In the context of an experiment such as that conducted for the S_VRAI project, irreversible anonymization, for at least the period of the study, is not desirable, as we shall see.

Physical persons consent certainly allows data to be collected and processed. But one should firstly be transparent with regard to the drivers, as has been described above, and, secondly, take organizational and technical measures to ensure privacy and data security. Among the tools available are pseudonymisation of identifying data and the partitioning of data access. Finally, the security measures taken should prevent illegitimate intrusions.

Pseudonymising when anonymizing is not possible

In 2009, the European data protection data controller issued a reminder that *"for personal data to be processed anonymously, no-one, at any stage whatsoever of the processing - taking into account all means reasonably likely to be used either by the processing* data controller *or by another person - must be able to link the data considered to an identified person"* (notice of July 22, 2009 on the ITS draft directive of 2010). The European working group on data protection (G29) stressed in turn that the use of anonymous data should be preferred whenever possible [4, 17]. Deletion of nominative data does not guarantee that there will be no identification and that the link between the data and the person concerned will be broken.

In addition, to carry out this type of experiment researchers have to know some identifying data, or even personal data:

– Material implementation of the experiment requires knowledge of the vehicles in which the EDRs are installed (to manage the fleet of recorders, fit them and maintain them). When a vehicle is used by only a limited number of drivers (or even just one), the data reported by a vehicle can easily be associated with a driver. Procedures should therefore be set up to limit the risk of indirect identification.

– Road safety research sometimes makes it necessary to collect data, some of which are potentially identifiable, if only indirectly or by cross-referencing them. For example geolocation for traceability or profile data such as gender, age, driving experience, etc. Such data were collected in S_VRAI using a magnetic card as explained above.

To enable these magnetic cards to be managed, correspondence tables were kept for the duration of the collection and managed by team members who did not have access to the data collected.

For the analyses themselves, potentially identifying data were pseudonymised by encryption. All data were encoded and compressed. Data that could be used to identify the driver directly, such as name and date of birth, or indirectly, such as the vehicle identification number or EDR serial number, were encrypted using a hash algorithm.

Pseudonymisation guarantees a certain level of confidentiality with respect to third parties and staff. But it does not guarantee that the person will remain anonymous or even that it will be impossible to reidentify him/her. Informed consent then becomes important. That is why each volunteer was informed about the project together with his/her right to access their own data and their right to erasure.

Compartmentalizing data access and confidentiality

In organizations likely to host data, one aspect of security is the possibly contractual requirement of confidentiality, (written undertakings, rules etc.). In the S_VRAI project, two types of partition were set up: one with regard to the line managers of volunteers, who had no right of access to data, the other with regard to the project partners. Each partner had limited access to the data needed to conduct the study he was in charge of.

Line managers, just like the people who performed the studies, signed non-disclosure agreements individually.

This separation was designed to limit access to the data solely to the research teams who needed them to carry out the studies. This partitioning was all the more essential because the fleets taking part were under the responsibility of services whose staffs were also taking part in the studies.

Securing the data access chain against unlawful intrusions

Security is justified by two objectives that can be achieved by implementing technical measures.

The first is the right not to be recognized when this is not necessary, by people who have no right to learn personal data. All measures must be taken by the processing data controller to preserve data security (1978 law, Art.34).

The second concerns the prevention of intrusion by unauthorized persons, particularly for malicious purposes which could have consequences not only in terms of capturing driver data but also in terms of accident risk.

The security of servers, networks and terminals (sensors, EDRs, research staff's computers) should be as reliable as possible to prevent these intrusions. Technology can be used to create the conditions for this security.

These aspects were taken into consideration at all levels of the collection and processing chain in the S_VRAI project. The measures deployed were evaluated by a state agency which issued a statement concerning data security. This statement warrants that the data is protected all the time that it is being transferred and processed, from storage in the EDRs to hosting in IFSTTAR and Cerema servers, via transfer through the telecommunications system.

The "right to be forgotten"

The "right to be forgotten" is not expressly covered by French or EU law. In the digital world, this is sometimes illusory [18]. It has not been sanctioned in the latest version of the future European regulation but the "right to erasure" was enhanced (Art. 17). Some of the measures included in the 1978 law (Art. 6.5 °) and in directive 95/46/EC (Art. 12b) show that the legislator is already sensitive to this aspect. It is not possible to store data in a form allowing identification of people beyond the time necessary to achieve the objectives. For example, when examining the e-call system, the CNIL imposed data erasure as soon as they had been used for purposes of assistance and relief (2010-096 deliberation of April 8 2010, above).

In the S_VRAI project, erasure of identifying data and correspondence tables was imposed as of the end of the research. Nominative data were deleted as soon as possible. In some cases, they could be stored in completely separate files from the processing files, for example for archiving or storage in case any legal dispute should arise.

4. Conclusion

Applying all of these conditions meant that the project could be completed in a context of confidence with respect to the different people involved:

– the drivers, who agreed to entrust us with their data. Having obtained authorization from the CNIL confirming that all the security and privacy measures had been taken was sometimes a decisive factor for people agreeing to participate in the experiment;
– the road managers who showed their interest;
– the CNIL, which issued an authorization in respect of:
  - the legality of the goals and the legitimacy of those invested with a public service mission to help prevent road risks;
  - the implementation of measures to guarantee the right of volunteer drivers, clearly informed beforehand about the initiative.

The measures adopted may be regarded as an example because they are related to an experiment that produced significant results in terms of knowledge of road risks related to infrastructure as part of the S_VRAI project. This project also showed that it was possible to conduct this type of study in compliance with the rights of the people concerned, by taking these rights into account as of the design stage. In addition to research projects, the framework defined by the researchers can also be tested in the context of the deployment of connected vehicles. The framework deployed in the S_VRAI project meets with the concepts of *Privacy by design and by default* that will be imposed by the European Regulation from 2018; the security measures meet with current requirements that will be consolidated by the cybersecurity directive proposed in February 2013 by the European Commission, approved in December 2015 by the Council, which should come into force in 2018 as Regulations on the protection of personal data

The legal and technical framework proposed by the research team could therefore be used as a basis for conducting a similar experiment in Europe. Because it creates a precedent, this approach can also be considered a favourable method for building confidence in volunteers involved in this type of experiment; this trust is becoming increasingly essential in view of changing technologies on board vehicles.

5. Acknowledgements

The authors would like to thank the French government, Road Traffic and Safety Directorate which partly financed the S_VRAI project.

References

1. Guo, F., Fang, Y. (2013). *Individual driver risk assessment using naturalistic driving data,* Accident Analysis and Prevention, 61, 3-9.
2. Hallmark, S., Tyner, S., Oneyear, N., Carney, C., McGehee, D. (2015). *Evaluation of driving behavior on rural 2-lane curves using the SHRP 2 naturalistic driving study data*, Journal of Safety Research, 54, 17-27.
3. Hynd, D., McCarthy, M. (2014). *Study on the benefits resulting from the installation of Event Data Recorders,* TRL Report, PPR707, European Commission, DG MOVE, 224p
4. IWGDPT (2011). *Event data recorders (EDR) on vehicles - Privacy and data protection issues for governments and manufacturers.* Final Draft 675.42.10 4 April 2011.
5. Ledoux, V., Subirats, P., Violette, E., Bonin, Y., Serre, T., Naude, C., Guilbot, M., Lechner, D. (2014). *Using event data recorder to detect road infrastructure failures from a safety point of view*, AET/European Transport Conference 2014. 29 sept-1st Oct, Francfort, Deutschland.

6. Serre, T., Naude, C., Chauvet S., Fournier, J-Y., Lechner, D., Ledoux, V. (2014). *Causes of road incidents,* Transport Research Arena (TRA), Paris, France, April 14-17.
7. Lechner D., Thomas D. Naude C. *Projet EDR. Enregistrement des données des évènements de la route. Conception et pré-industrialisation d'EMMA/2*. Rapport final, convention DSCR-INRETS (ex. IFSTTAR) n°0003629, juin 2009.
8. Goegle J.-P. Chronique du droit « post-Snowden : la CJUE et la CEDH sonnent le glas de la surveillance de masse/ La Revue des droits de l'Homme. Actualités Droits-Libertés. http://revdh.revue.org/2074
9. CNIL (2012). Vie privée à l'horizon 2020. Paroles d'experts. Collection Cahiers IP, Innovation et prospective n°1
10. Article 29 Data Protection Working Party, "Opinion 4/2007 on the concept of personal data," 01248/07/EN WP 136, adopted on 20th June, 2007.
11. Article 29 Data Protection Working Party, "Opinion 13/2011 on Geolocation services on smart mobile devices," 881/11/EN WP 185, accepted on 20th June, 2011.
12. De Montjoye Y.A., Hidalgo C.A., Verleysen, M& Blondel V.D. (2013) . Unique in the Crouwd:theprivacy bounds of human mobility. Nature Scientific reports, 3, 1376; DOI:10.1038/srep01376
13. Türk A. La vie privée en peril. Ed. Odile Jacob, 2011
14. Article 29 Data Protection Working Party, "Working document on data protection and privacy implications in eCall initiative" WP125, adopted on 26th September 2006
15. Ferrandez, F., Brenac, T., Girard, Y., Lechner, D., Jourdan, J.-L., Michel, J.-E., Nachtergaele, C., (1995). L'étude détaillée d'accidents orientée vers la sécurité primaire. Presses de l'École Nationale des Ponts et Chaussées
16. Article 29 Data Protection Working Party, Opinion 15/2011 on the definition of consent. WP187, adopted on 13 july 2011
17. Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques. WP 216, adopted on 10 april 2014
18. Dupont-Lassalle J., (2015) « Beaucoup de bruit pour rien ? La précarité du « droit à l'oubli numérique » consacré par la Cour de justice de l'Union européenne dans l'affaire Google Spain (obs/s. C.J.U.E., Gde Ch., arrêt Google Spain SL, 13 mai 2014) », RTDH, n° 2015/104, p. 987