université angers

Granem
Groupe de Recherche ANgevin
en Economie et Management
UMR-MA n°49

13, allée François Mitterrand
BP 13633
49100 ANGERS Cedex 01
Tél. : +33 (0) 2 41 96 21 06

Web : http://www.univ-angers.fr/granem

Young Europeans' motivations, perceived risks and requirements regarding electronic identification : Some comparative results from focus groups in four EU27 countries

Caroline Lancelot Miltgen
GRANEM, Université d'Angers

Décembre 2010

Document de travail du GRANEM n° 2010-2-024

AGRO CAMPUS OUEST

Young Europeans' motivations, perceived risks and requirements regarding electronic identification : Some comparative results from focus groups in four EU27 countries

Caroline Lancelot Miltgen
Document de travail du GRANEM n° 2010-02-024
Décembre 2010
Classification JEL : O3, M15, M16.

Mots-clés : Identité, données personnelles, identification électronique, dévoilement de soi, vie privée, etude qualitative
Keywords: Identity, personal data, electronic identification, self-disclosure, privacy concerns, qualitative study

Résumé : La société de l'information dans laquelle nous vivons a - dans la plupart des cas - augmenté le problème central de l'accès aux informations de nature personnelle. Jusqu'ici, peu de travaux se sont intéressés aux perceptions des individus-citoyens (à la fois en termes de risques et de motivations) quant 1/ au dévoilement de données personnelles en ligne et 2/ à l'adoption de systèmes d'identification électroniques spécifiques (tels que la biométrie) en particulier. Ce papier présente les résultats d'une étude qualitative - deux réunions de groupes ont été menées dans quatre pays européens différents (France, Espagne, Allemagne et Royaume-Uni) - visant à mieux comprendre les motivations, les risques perçus et les exigences des jeunes citoyens européens (15 à 25 ans) concernant l'identification électronique et le dévoilement en ligne. Au total, 76 jeunes ont participé à ces réunions de groupe. Les discussions ont été retranscrites puis traduites en anglais avant d'entreprendre une double analyse textuelle utilisant les logiciels Alceste© et Wordmapper©. Les résultats des deux analyses textuelles montrent des ressemblances et des disparités au sujet des perceptions des jeunes Européens en matière de dévoilement de données personnelles en ligne et d'intention d'adoption de technologies d'identification. Les similitudes se rapportent en particulier 1/ aux risques perçus quant à la collecte et à l'utilisation de données personnelles en ligne ; et 2/ au manque de connaissance envers la réglementation en vigueur et de confiance envers la puissance publique. L'analyse comparative confirme les différences culturelles dans ce domaine mais montre également des points communs entre les quatre pays analysés. En conclusion, la plupart des jeunes interviewés voudraient plus de contrôle et de réglementation concernant les données qu'ils fournissent sur Internet. Des implications pour les universitaires, les praticiens et les décideurs politiques sont fournies.

Abstract: Moves towards an Information Society have, in most cases, enhanced the central problem of control over access to identity information. Until now, there has been little research concerning peoples' perceptions (both in terms of risks and motivations) towards 1/ electronic identification (i.e. electronic disclosure of personal data) 2/ the adoption of some specific electronic identification systems (such as biometrics) in particular. The paper presents the results of a qualitative study - two focus groups were run in four European countries (France, Spain, Germany and the United Kingdom) - aiming to better understand young European peoples' (15 to 25 year olds) motivations, perceived risks and requirements regarding electronic identification and online self-disclosure. In total, 76 young people took part in the focus groups. The discussions were transcribed and then translated into English before undertaking a double textual analysis using Alceste© and Wordmapper© software. The results from the two textual analyses show both resemblances and disparities concerning the perceptions of young Europeans in relation to personal data disclosure online and adoption of identification technologies. The similarities more particularly relate to: 1) the perceived risks related to the collection of personal data on line; and 2) the lack of knowledge and confidence towards public regulation. The comparative analysis confirms the cultural differences regarding these topics but also shows some similar views. Finally, most young people interviewed would like more control and better regulation concerning the data they provide. Implications for academics, practitioners and policy makers are provided.

Caroline Lancelot Miltgen
Faculté de Droit, Economie et Gestion
Université d'Angers
caroline.miltgen@univ-angers.fr

This study was funded by the European Commission IPTS (Institute for Prospective Technological Studies) Joint Research Centre: EC JRC Contract IPTS n° 150876-2007 F1ED-FR (December 2007 to November 2008, budget: 57000 Euros) with Caroline Lancelot Miltgen as the research project leader at the University of Angers (France).

1. Introduction

With the introduction of digital media, publicly available networks and the development of the Information Society, identity has become a pressing contemporary issue with wide ranging implications (Asaro 2000, Fountain 2000, Grijpink 2002, Hyder 2005, Nash & Lejeune 2010). Information Technology (IT) has revolutionised the collection, processing and use of identity information since more data can be collected, stored and processed into usable information (Wang & Taratorin 2010). Moves towards an Information Society have consequently, in most cases, enhanced the central problem of control over access to identity information (Hoadley 2010, Wang et al. 2010, Ward & Smith 2002).

As a result, identification in the context of emerging technologies has become a major area of research. More specifically, it concerns the study of both the conception of such electronic identification (eID) systems (e.g. biometrics and RFID technologies) and their acceptance as systems permitting self identification while surfing the Internet for commercial and/or administrative purposes. Both academics and practitioners agree that such identification technologies can not succeed if the people using these tools for identification purposes are not: 1/ fully aware of the specific advantages and risks of these systems; 2/ able to control the use that is made of the identity data (Kim 1995, Ratha 2001). However, until now, there has been little research, especially in the information technology literature, concerning the peoples' perceptions (both in terms of risks and motivations) towards 1/ electronic identification in general (i.e. electronic disclosure of personal data) 2/ the adoption of some specific electronic identification systems (such as biometrics) in particular. This study seeks to overcome that deficiency by reporting the results of a qualitative study of young Europeans motivations, perceived risks and requirements on future electronic identification systems. For the purpose of this study, we define motivation as the driving force (intrinsic or extrinsic) which causes the individual to achieve goals (here to adopt an identification system or to disclose personal data on the web). Risks concern the deviation of one (or more) results of one (or more) future events from their expected value. Technically, the value of those results may be positive or negative. However, general usage tends to focus only on potential harm (e.g. privacy or security failure) that may arise from a future event (e.g. data misuse), which may accrue either from incurring a cost (loss of privacy) or by failing to attain some benefit (e.g. automatic authentication). Risk perception refers to the subjective judgment that people make about the characteristics and severity of a risk (here mostly a privacy risk). Finally requirements regarding electronic identification systems refer to documented needs of what the eID service should be or perform (e.g. security).

This study investigates what members of the young European public think about issues of identity, privacy, self-disclosure, protection of personal data, and use of electronic identification (eID) systems. The research comprises a series of interview groups with the young (15-25 year olds) European public, in four different EU27 countries (France, UK, Spain and Germany). Young people were chosen for interview as they embrace cutting edge information technologies in large numbers and represent possible opinion leaders in the area of IT (Akman & Mishra 2010). Moreover, as they have grown up with these new technologies, they undoubtedly better reflect the behavioural patterns of society in the future since: 1) they are the future adult citizens; 2) they have a high level of IT literacy; 3) they tend to grasp new technologies rapidly (Buckingham 2008, Eysenck 1974, Hulicka & Weiss 1965, Palfrey & Grasser 2008). Additionally, as young people aged between 15 and 25 years make up 11 to 16% of the European population (Eurostat data, 2008) depending on the country considered, they represent quite a large part of the population.

2. Foundations and purposes of the research

The main surveys and studies that were carried on the subject of ICT and eID systems at the moment have shown that there is no clear conclusion about:

- What people think about ICT in general, electronic identification systems and applications (such as electronic cards, RFID technology and biometrics) in particular?
- What the main motivations and perceived risks are in adopting such electronic systems?
- Whether the public is ready (or not) to adopt such electronic identification systems?
- What the specific needs and requirements of the public are, concerning such systems?

One objective of the study was to focus on young European peoples' perceptions about personal data disclosure and eID systems in order to provide some answers to these questions.

Typically, whatever the country considered, contradictory perceptions on ICT and electronic identification exist. Technologies are not always seen as dangerous or risky, but most citizens require reassurance on security and privacy, personalisation of services, ease of use and content quality before adopting them. Privacy is one of the most important requirements (Jung 2009, Magkos et al. 2009). However, although consumers routinely declare that they value their privacy highly, they do not seem to actively incorporate privacy concerns in their transactions. The ability to remain anonymous, to specify who can view and use information, privacy policies and security icons are very important to most people, but very few frequently use control techniques before logging in (and on social networking sites in particular) and many people use their real identities when registering on Websites (Fogel & Nehmad 2009; Jensen, Potts & Jensen 2005; Paine et al. 2007). This so called 'privacy paradox' has been acknowledged for many years (e.g. Gross and Acquisti 2005, Oomen and Leenes 2007) and although some explanations and possible causes have already been proposed (e.g. Norberg, Home and Home 2007), academics, practitioners and policy makers need a more complete picture.

A successful deployment strategy for new eID systems requires that privacy interests are balanced with the benefits that advanced services may offer (Meziane & Benbernou 2010). This explains the need to investigate the extent to which people are aware of new identification means, perceive their costs (risks, privacy and confidentiality) and benefits (relative perceived value) and intent to adopt them. This study therefore explores, to a greater extent how young people consider their identity and manage personal data online. The aims of the study are to: 1/ understand how people differentiate between identity and personal data, 2/ understand what makes people decide to self-disclose and/or adopt electronic identification systems and 3/ evaluate the importance and the causes of the "privacy and identity paradoxes".

Trust is also a key success factor for the implementation and acceptance of ICT applications (e.g. Mezgar 2003). Building trust in the citizen and end-user could be a key success factor for the eID innovation to be adopted. Existing studies show that the majority of the population (even in Europe where specific data protection laws exist) is unaware of 1/ the risks posed by the collection and use of personal information, 2/ their rights concerning the protection of their privacy and 3/ effective technologies or control tools that should help them to protect their privacy (Senicar, Jerman-Blazic & Klobucar 2003; Ricci 1998). Most people also feel that they can't find out what actually happens to their personal data. As a consequence, most people do not trust institutions' competencies to handle their private details (e.g. Backhouse & Halperin 2007). Trust in 1/ organisations' collection and use of citizens' personal information – whether for administrative and/or transactional purposes - and 2/ in governments' ability to regulate the circulation of data will be examined in this study. The paper also explores the extent of people's knowledge, use and perceptions of public regulatory and other protection means to ensure privacy and security.

3. Research method

3.1 The choice of discussion groups

The qualitative method of analysing discussion groups was used in this research. This method appears as a useful tool to promote dialogue between all participants around various issues associated with electronic identification systems, online self disclosure and personal identity data management (PIDM).

Two discussion groups of between 8 to 12 participants aged 15-25 were conducted in four EU27 countries (i.e. Spain, France, Germany and Britain). The aim was to investigate what young Europeans think about identity, protection of personal data, security, privacy and eID systems issues. The main objective was to allow youngsters to express themselves on these topics and to let them talk about their motivations or reluctance to adopt such new electronic applications. Their perceptions of the risks to give personal details in these contexts - and more particularly for online applications - were also taken into consideration.

People's engagement and responses to key issues and principles associated with identity and identification was examined. By studying the process through which people encounter and assimilate such material, light was shed on how public perceptions are formed and maintained, especially on the reasoning that people use to make sense of regulation and control systems.

The value of the technique and its role in bridging social and cultural differences lies in discovering unexpected findings, often obtained from a free-flowing discussion that is respectful, and not condescending to participants. The group discussion approach has other advantages (Gelula 1997, Lago et al. 2007, Semeonoff 1952). First, for a topic such as eID where prior public awareness and knowledge is likely to be low, it allows people to engage in a real discussion without fear of being judged or social desirability bias. Second, the discussion groups are facilitated by the interviewers, who enable participants to express themselves and develop their views and ideas about the issues they feel important, interesting or puzzling. Third, it provides an opportunity to examine how participants' views develop at an individual or group level over the course of the discussion groups.

3.2 The participants

Although not a 'representative sample' in quantitative terms, participants in the study were diverse in nationality, gender, age, "professional status", education level and Internet skills. Moreover, we tried to ensure a balance of all of these variables. In this respect, the results from this study can be considered as meeting Mason's (1996) concept criteria of being 'theoretically generalisable'. This requires that: 1/ that our sample of participants is not specifically atypical (e.g. all middle class, or all men); 2) that the analysis has been rigorous and systematic. Both conditions are verified here (see table 1 for the verification of the former criterion). In respect of these points, the findings presented here can be taken as an indication of current young European (i.e. French, English, Spanish and German) people's attitudes towards online disclosure and identification systems, although not the quantitative distribution of those attitudes.

Table 1 Repartition of population in Eurostat 2008 and in our study

	France (%)		**UK (%)**		**Spain (%)**		**Germany (%)**	
	Eurostat	Study	Eurostat	Study	Eurostat	Study	Eurostat	Study
Gender								
Male	51	60	51	53	51	50	51	50
Female	49	40	49	47	49	50	49	50
Age								
15-18	36	22	36	20	33	45	35	22
19-21	28	34	28	40	26	17	28	28
22-25	36	44	36	40	41	38	35	50

3.3 The focus groups

Focus groups ran for approximately one and a half hours and were conducted by a qualified researcher specialised in qualitative research and/or in one of the topics studied (i.e. ICT, privacy). All moderators used the same topic guide that had previously been translated in the different languages. Participants (76 in total) were asked for their views on the perceived advantages and disadvantages of eID technologies and for their reactions to self-disclosure, security and privacy issues when giving personal details for identification purposes. They were also asked about protection and regulatory issues. All focus groups were audio and video recorded, transcribed and translated into English, in order to make useful comparisons between the discourses. They were then analysed to capture the key points, positions and opinions.

3.4 Data analysis methods

Two different kinds of analysis were carried out. First, we used a ‘classical’ content analysis, the prime objective of which was to reduce the data, summarise and organise the information according to the rules derived from existing theory. Content analysis consists of discovering the main ideas and topics discussed by the participants which correspond to the main important issues discussed. Then, a “discriminate” analysis was conducted to see if some differences existed in the discourses of the participants according to socio-demographic variables (e.g. according to their country of origin).

The data analysis methodology used here is based on the Statistical Textual Analysis. Statistical Textual Analysis is itself based on lexicometrics, mainly used to count words and forms. The basic hypothesis is that language levels and text structure can be inferred from recurrent distributions of words. The use of statistical methods of textual analysis offers an extremely rich exploratory approach, both for the comparative study of texts and for the comprehension of the content. This type of application is well-established and its effectiveness is widely acknowledged (Lebart and Salem, 1988). The textual statistics are a valuable tool for the reading and comparison of the transcriptions. Their application to the field of marketing and IS research emphasises their potential and the results that can be obtained (Gauzente and Peyrat-Guillard, 2007).

Analysis of textual data is based on a multidimensional descriptive analysis of texts, involving mainly factor analysis of correspondence and automatic classification, applied to the lexical profiles of the texts.

Qualitative data analysis using specific software involves an interactive cycle of reflection and innovation. As it permits the manipulation of the data more efficiently, the purpose of such software is to help the researcher: 1/ to analyse data in a systematic and thorough manner, 2/ to identify patterns and interconnections and 3/ to develop or test a theory.

Computer programs for textual analysis are numerous. Alceste© was an obvious first choice because this software is the most widely-used in the field of research (Reinert, 1986). This program proceeds by studying the formal structure of the co-occurrence of the words in a given corpus. In practice, a classification of the answers according to the similarities and differences in the participants’ vocabulary is obtained. To complete the analysis and test the stability of the results, WordMapper© (GrimmerSoft) was also used, which offers a complementary view of the clusters.

In summary, software packages such as the ones used offered following advantages:

- *Speed:* the speed at which such programs can carry out sorting procedures on a large volume of data is remarkable. This allows more time to analyse the meaning of the data, enabling rapid feedback of the results.
- *Rigor:* rigor adds to trust in the research findings. In the context, it has meant counting the number of times certain words occurred as well as selecting anecdotes that supported our interpretations.

- *Sampling*: as more time was spent on creative tasks, a stronger analysis was developed. Descriptions and theories were used to strengthen the validity of the views by ensuring that sufficient incidences had been sampled.

3.5 The quality of the results

Ensuring the validity of a research consists of checking the relevance of the results (internal validity) and evaluating their level of generalisation to the whole population (external validity). The internal validity relates to the adequacy (i.e. relationship) between the observations (or results) and reality. It generally constitutes an advantage for qualitative research as it is possible to control some bias (e.g. bias of history, maturation, or mortality) and to corroborate the data and the results.

One way to verify the validity of the results consists of ensuring that the analysis is guided by a theoretical approach. This is why Yin (1989)'s advice was followed, which consisted of a systematic comparison between the empirical results and the theoretical proposals resulting from the literature. Confirming most of the results found in this study.

The external validity generally constitutes a drawback for qualitative research as it is more difficult to generalise the results than with quantitative research. One can only generalise the results to contexts identical to those covered in the qualitative phase. However, these contexts are often reduced. For example, in our analysis the context is limited to young French, English, Spanish and German people corresponding to the profiles of our respondents. Nevertheless external study validity amelioration is possible, by comparing the results with the literature (Eisenhardt, 1989). This makes interpretation of the results in different ways possible and allows the specificities of each interviewed individual or group to be exceeded. The results can then be generalised to cover a wider population. The diversity of the people interviewed (more than 70) in the study permits the possible generalisation of the results to the young population of the 4 countries covered (with all the necessary precautions).

Reliability consists of making sure that the research could be repeated by different researchers at different times with the same results. This method of defining reliability generally constitutes a drawback for qualitative research as confidence tests can not be employed. Moreover, this type of research is seldom "replicable" under the same conditions. There are several ways, however, to increase the "internal" research reliability. The first consists of running the discussions by complying with the elementary rules of interviewing (kindness, empathy, involvement, and sensitivity). This ensures that the data really correspond to the participants' thoughts. The second consists of ensuring that all interviewers use the same techniques and maintain a high quality when interviewing. All interviewers received an interview guide and detailed instructions[1] on 1/ the selection of the participants, 2/ interviewing techniques and 3/ how to conduct the discussions. This was to ensure that the interviewers all followed a similar procedure for recruiting the participants and conducting the interviews. At the end, it seems that all the interviewers maintained a high quality in their interviewing technique, if this can be judged by the similarity[2] of the results in all of the countries. During the analysis, various rival explanations for the representations described by the respondents were sought. Moreover, results were systematically compared with the maximum number of possible sources, in particular the studies and surveys on this topic. Finally, different kinds of analysis and software were used in order to ensure the quality of the results.

[1] Giving instructions for foreign interviewers is one of the 'accepted' methods for conducting cultural qualitative studies from a distance (Jacob Nielsen 1993).

[2] We refer here to the similarity of the results in their presentation (i.e. topics covered).

4. Main results

4.1 Perceived difference between personal data and identity

The discussions provide abundant details on how youngsters define identity and how they manage identity and personal data online. For example, the young people interviewed make a clear distinction between identity and personal data. Whereas personal data are mostly considered as public data accessible to everyone, identity mainly relates to all the personal data which can define a unique human being (e.g. civil status, ideology, personality, physical characteristics, etc...). For example, some French and Spanish participants clearly evoke this distinction between both concepts:

> '*Identity refers to all characteristics, everything that able use to characterize a person, everything that characterize a unique human being*'.
>
> *'Personal data is the written retranscription of identity. Identity is more the being'*
>
> *'The identity stays at the level of the concept, at the level of subjectivity whereas personal data are more an "objectivation" of this identity'.*
>
> *'Identity is more a relation of one person to another person. We discover someone's identity discussing with her; knowing her years after years. Conversely to personal data that are eventually a few persons who regroup data they know about one person, who establish general facts ... that are quite available to the knowledge of everybody'.*

Some German participants also make '*a difference between "real" online identities like those on StudiVZ and make up identities which you find in games like "Second Life".*

The use of the data is consequently of high concern for the young European people as identity is linked with a specific person and not to someone part of a marketing cluster.

4.2 Trust and risk perceptions about personal identity data management

The main drawbacks and risks perceived by the young European people surveyed in relation to the personal data they disclose on the Internet mainly relate to the following categories: identity theft and/or loss, loss of control (resale and reuse of information), financial fraud, harassment (numerous spam and advertisements), monitoring and loss of freedom. Here are some sentences focusing on these risks as perceived by youngsters:

> *'.. to be scared of having thousands of spam on our mailbox. I didn't want to … that one of my email account's ends up being full of arriving averts so that made me decide to use another one'. (France)*
>
> *'I remember ordering flowers for my girlfriend two years ago and it has been for two years that I have received their email every week. I remember I said "No I don't want" but they keep doing it". (England, Harassment)*
>
> *' I think probably the biggest risk would be somebody tapping into a bank account and taking money … fraud' (England)*
>
> *"I am afraid that my data could be freely accessible to other companies and could be misused". (Germany)*
>
> *It is mainly that I feel too much controlled and monitored. I just want to be free and in the case that I do not want to give my data away I want them to be safe. And I do particularly not want the state to have these data" (Germany).*

We should also take note that some people consider that there is no real or important risk or that these risks can be easily controlled.

> *'I'm not scared that my information will stand out. We know that yes we are taking risks, our information will be used for brands or for marketing surveys but finally … we accept it. Well it is how I accept it, I give my information, I know it will be used'. (France)*
>
> *'I think you have to weight it up, what is the likelihood of something happening? I have never heard of anyone having a bad experience. On the news, but not any friends'. (England)*
>
> *'I am quite accepting the risks because I think it is all personal choice. You could live a life without the Internet if you really wanted to … If you want to use it I think you have to accept the risks really if you want to use the facilities'.*

Globally, young European people have two main concerns in relation to the adoption and use of identification systems. These mainly relate to the use of personal data (privacy concern) and to the security of these systems (whether financial or technical). People seem to doubt frequently whether they can trust the organisation requesting their data and consequently use some criteria - such as logos and past experience with the site - to reassure themselves and to judge the trustworthiness of the other party. They also tend to have more trust in sites/organisations with higher reputations.

> *'I do not hesitate at all when buying goods from private companies and giving away my data. The reason is that serious companies want to treat me like a customer. Any other small company with a bad reputation would make me feel more uncomfortable." (Germany)*

As a consequence, to help people disclose data in a trustful way and encourage them to use eID system, the following recommendations - for both authorities and practitioners - emerge:

- limit the information asked and avoid asking sensitive data such as data in relation to health or finance (unless it is really compulsory for the transaction to be made)
- permit a clear identification of the organization – whether public or private – asking and/or using the personal identity data
- adapt the way the data is requested – whether online or on face-to-face interviews - to the target and to the sensitivity of the information
- secure the systems
- offer guarantees and reassurance by using fair information principles (logos, pictograms, privacy notices, …)
- adapt the regulatory framework to the specific needs and problems of the target and clearly inform/educate the citizens on the rights given by this regulation
- ensure freedom of choice and data control
- help everyone (citizens, companies, states) take ones own responsibility in data (mis)use

4.3 eID systems awareness

Whereas most young people talked about the advantages and drawbacks of the Internet, few have any idea of what eID consists. Moreover, although some are aware of the existence of electronic cards and passports, no one in the study had ever applied this technology. That is why discussing their motivations and perceived risks of adopting such systems was quite difficult for the participants. However, all were able to discuss the motivations and risks linked to the collection and use of their personal data for identification purpose and clearly request a better control on future personal data use. A German participant for example evoked both the advantages and drawbacks of a health insurance eID card:

> *'Generally speaking I do not care whether my data is saved on a chip, as long as I can voluntarily decide who can read the data. Otherwise I do consider it a safety hazard. Coming back to the saving of data on identity cards, right now there is a discussion going on about saving data on your health insurance cards. And I think that this system might have a lot of advantages, since e.g. taking multiple x-ray pictures, etc. can be avoided with this kind of system. However, it is only a good solution if the data are saved locally on your card but not on a centralized system'.*

Other participants insisted in the multiple risks with this system especially as it concerns very sensitive data:

> *'For me it is rather a question of who can read and get the data. And since medical data is more sensitive than a finger print I have great concerns about the risks'.*
>
> *'An example might be that a health insurance company has access to the data about our health. This creates a chance to misuse the data to, for example, exclude people from health insurance because of their increased risk of getting an illness'.*

Whereas most participants recognise the high risks of eID technologies as personal data can be stolen or misused, some however recognize that it will be difficult not to use such systems if you don't want to be excluded from the digital society:

> *'This discussion is about whether electronic identity cards should be introduced. This however seems to be too risky in my opinion. I would be afraid that much data could be stolen and misused. I do not see however any problem in saving details like my fingerprints on my passport'.*
>
> *'I think it is very difficult not to use the modern identification technologies. If you did so you would exclude yourself completely from the use of the internet'.*

The results were thus useful to obtain people's impressions about identification systems in general, although not always clearly linked with a specific eID technology (e.g. biometrics, RFID or electronic cards/tokens...).

4.4 Control, protection and regulation in relation to privacy

Knowing the importance of risk and the lack of trust evoked by the participants, the adoption of identification systems requires 1/ more control on the use of personal data and 2/ better protection against possible misuse. However, whereas European legislation could be an efficient protection tool, few young European people seem aware of the legal protective measures offered and many seem sceptical concerning the efficiency of such legislation. And this is almost true in the four countries surveyed. Below are some examples of sentences:

> *'I don't think there are any laws from the European Union. I imagine there are but they are not enforced. The Internet can't really be enforced'. (England)*
>
> *'I don't know about the specific legislation but I know that information online in controlled. For instance, talking about mails, if you send a message containing the words "bombs, fatal and tower", this mail will be controlled'. (Spain)*
>
> *'I think it is pretty clear to everyone that there is a Data Protection Act. But I think that nobody really knows the exact regulations of this law. This is something for jurists and lawyers'. (Germany)*
>
> *'I think it is good that there are regulations and laws that protect consumers. Which regulations there are exactly? I do not really know, though'. (Germany)*
>
> *'Legislation should exist before the problems appear and in fact it is always the other side and therefore legislation always arrives too late'. (Spain)*

One participant evoked the digital divide as regards need for better control and regulation:

> *'Well, in these things, security and privacy are not guaranteed, but I think the perception depends on the age. For instance, at the moment, I am an adolescent and I don't want to be controlled but I know once I become a father I would like to control my children' (Spain)*

Some participants also notice the limit of national or regional regulatory framework such as the one proposed in EU27:

> *'Law is a geographical characteristic. The Internet … it's worldwide. So there is probably some kind of interaction that needs to be done and all hasn't been done'. (France)*
>
> *'I think the implementation of such laws will be difficult since we are talking about an international context e.g. talking about the Internet'. (Germany).*

Globally, findings point to an overall negative perception of the authorities by the participants, confirming results obtained by Backhouse and Halperin (2007). The vast majority of the respondents do not trust the public institutions; they are seriously critical about the competence of the authorities, and are dubious about their ability to handle personal data. Some participants are suspicious of the authorities misusing their data (mainly in the French sample), whereas others have more trust in public authorities than in private companies:

> *'For example, when they make surveys on how much time you watch TV, if you write 30 hours per week and you declare that you don't pay the TV licence fee. I think that if the state collects this information and comes to you the next day, it is an intrusion in your private life'.*
>
> *'Personally, I think that it is even worse to the State because there is a risk of occupation from the political parties'.*
>
> *'I rather gave my data to public authorities than to private companies. I think that both aspects are of great importance. On the one hand the disturbing phone calls, spams, etc. and on the other hand the argument that my data could be in the hands of someone who misuses it'.*
>
> *'I felt safer giving my data to a public authority than to a private company. This thought however was based on the assumption that I thought private companies might have rather more reason to misuse my data.'*

It seems thus very important for the authorities – both at the EU27 and at a country level - to communicate more efficiently concerning this legislation, so that the citizens are informed and reassured about the protection offered. Some participants propose for example that the legislation be taught in school:

> *'I think it should also be taught in school, since it is increasingly important in today's life. Unfortunately most people are not well informed enough.'*
>
> *'I think it should not be so difficult to inform pupils also about the Data Protection Act. It's already obligatory to study the basic Constitutional Law'.*
>
> *Yes, I think the State has the duty to inform its citizens. This might already take place in schools'.*

4.5 Similarities and differences in public perceptions

This part is concerned with the presentation of the main similarities and differences between the countries. Measuring similarities and differences in the public perceptions is an important step in a study such as this. As the people interviewed come from different countries in Europe (and these countries come from the same EU27 regional block: the west of Europe), studying the cultural similarities and differences constitutes an important focus point (Almeida, Pais & Formosinho 2009).

Globally, in each country the main topics evoked by the participants relate to:

- Informational privacy (i.e. collection and use of personal data)
- Security and protection
- Risks attached to the (mis)use of personal data and identity
- Control and regulation

Findings also show that: 1/ the risks relative to the adoption of new eID technology are particularly linked with security (e.g. prevention of fraud) and privacy (protection of personal data) 2/ most users require specific protection in order to counteract these specific perceived risks, whether offered by the technology (e.g. passwords) or by the law/police. However, a general scepticism was found in all the countries concerning the capability of the public authorities to regulate the use of personal data in general and of eID systems in particular.

Despite these similarities, there are also differences between the people that deal with:

- The importance of identity and privacy
- The level of awareness concerning eID applications and specific legislation
- The importance of control and security measures
- The level of trust accorded to public and private organisations in dealing with the data
- The role of public authorities in ensuring protection of personal data

Table 2 hereafter, shows the main vocabulary[3] used by the participants in each country.

This table shows that the French participants interviewed mainly focus on identity and personal data (collection with questionnaires and use of). This importance of identity is also seen in the Spanish sample which mainly focuses on identification (e.g. identified/identify). The French also evoked the importance of the relationship between people, the user and the organisation which collects the data. This importance of the relational aspect can also be found in Germany where the participants mainly evoked the importance of a "network". Although both French and German people insist on the importance of the relationship, the Germans also evoked the importance of a guarantee (e.g. insurance, reputation) which should mainly come from the government (e.g. authorities, regulation). Whereas this regulatory aspect is not evoked in the French sample, it also appears in Spain (e.g. legislation, institution) and in England (government, police). German people also evoked the potential risks incurred in using new technologies (e.g. afraid, misused) and insist on the importance of security measures (e.g. safe/safety).

[3] Results are given alphabetically and not according to the importance of the word.

Table 2 Main vocabulary used in each country

FRANCE	ENGLAND	SPAIN	GERMANY
- identity - information - personal - questionnaire - relation	- bank - cautious - compromised - disadvantage - European - Facebook© - fraud - government - hacked - passport - password - police - risk - trusted - worried	- card - confident - controlled - credit - freedom - identified/identify - institution - legislation - lie - privacy - technologies	- afraid - authorities - (phone) calls - company - data - insurance - misused - network - regulation - reputation - safe/safety

England and Spain both evoked the problems/risks of online banking and payment. But whereas the English people seem quite concerned by these problems, the Spanish seem more confident (e.g. confident, freedom). Despite this trust however, the Spanish are the only Europeans who spoke privacy (i.e. protection of personal data) and the possibility of lying.

Finally, the potential risks incurred in using ICT and eID systems in particular are mainly underlined by the English people (e.g. compromised, disadvantage, fraud, hacked, risk, worried) who thus insist on the protection measures needed to lower these risks, whether offered by the government (e.g. police) or technology (e.g. password).

Globally, we can see that each country can be close to or different from another country depending on the topic studied. Indeed, the answers from the French and German samples were similar for the relational aspect (i.e. creation of a network) and different for the necessary involvement of public authorities. The same is true for England and Spain, their perceptions being similar for the issue of online banking and online payment security and different for the level of trust/confidence and the issue of privacy.

4.6 Comparison of both analyses

In order to ascertain the quality of the results the two programs (Alceste© and WordMapper©) are compared. If the main conclusions obtained with the first software are confirmed by the second, the validity of the results will be ensured as the triangulation of the data - whose merits are advocated by several qualitative researchers (e.g. Eisenhardt 1989, Nau 1995, Tashakkori and Teddie 1988) - will be guaranteed. If this is not the case, any conclusions drawn from the data will have to be considered with caution.

Table 3 hereafter shows the results obtained in both programs and can easily compare them.

Table 3 Comparison of countries' differences found in Alceste© and WordMapper©

	ALCESTE©	WORDMAPPER©
FRANCE	- Values the privacy and security of their data - A bit pessimistic concerning the control they have over their personal data - Do not seem to believe that the authorities can protect them efficiently - Seem quite unaware about the existence and characteristics of eID systems	- Mainly focus on identity and personal data (collection and use of) - Importance of the relationship between the user and the data collecting organisation - Regulatory aspect is not evoked in the French sample: seem less concerned by regulation and public intervention to regulate the use of data and eID systems
ENGLAND	- Very cautious about the use of their data and seek signs that can reassure them before self-disclosing - Seem quite aware about the existence of eID systems and about their advantages and disadvantages	- Quite concerned by these problems - Underline the risks incurred in using new ICT in general and new eID systems - Insist on the protection measures needed to lower these risks, whether offered by the government (e.g. police) or the technology (e.g. password)
SPAIN	- Seem quite insecure concerning the security of their data - Find that the collection of data is now more (and too) systematic and that the legislation has to adapt to this evolution - Value all the advantages of the Internet and find that it is a good way to communicate with others although the communication becomes more impersonal	- Seem more confident (e.g. confident, freedom). - Speak about privacy (i.e. protection of personal data) and evoke the possibility of lying - Mainly focus on identification (e.g. identified/identify)
GERMANY	- Value the Internet as a communication tool and a way to build a social network - Very concerned about the (mis)use of their personal data (reported cases of fraud) - Differentiate between public and private organisations - Do not seem really aware of the regulatory scheme that exists in Europe and seem quite sceptical concerning the abilities of the governments to regulate the Internet - Will adopt new eID systems only if they can control the use made of their personal data	- Mainly evoke the importance of a "network" - Evoke the risks incurred in using new technologies (e.g. afraid, misused) and insist on the importance of security measures (e.g. safe/safety). - Evoke the importance of guarantees (e.g. insurance, reputation) which should mainly come from the government (e.g. authorities, regulation)

This table confirms that the results are quite similar for both analyses and thus the quality of all the outcomes of this study is confirmed. Below these similarities are detailed.

With Alceste©, young French people seem quite pessimistic concerning the control they have on their personal data. They value the privacy and the security of their data but do not seem to believe that the authorities can protect them efficiently (they almost never talk about the authorities and do not evoke the laws that should protect them). This result is confirmed with WordMapper© as no word linked with regulation and authorities was found in the main vocabulary used by the French people.

Alceste© also found that, unlike the French, the young English seem quite aware about the existence of eID systems and about their advantages and disadvantages. This result is also confirmed by WordMapper© as many words linked with risks and technology were used in the English sample (e.g. compromised, disadvantage, fraud, hacked, risk, worried).

The Alceste© analysis concludes that the young Spanish people seem rather more confident (than the young people from the three other countries) concerning the security of their data. This report is also confirmed by the WordMapper© results as the Spanish were the only people who evoked the words “confident” and “freedom”.

That young German value the Internet as a communication tool and a way to build a social network was founded in both results. Both software packages also found that young Germans identify a real difference between public and private organisations concerning the use of personal data. In both results, German people evoked the intervention of public authorities to regulate the use of new technologies but it seems quite difficult to conclude whether they value public intervention or not.

5. Conclusion

With these results that have proven high convergence with both methods used, a conclusion can now be made with implications, some limitations and perspectives of future work on this topic.

5.1 Implications

The study is expected to have significant scientific, pragmatic and policy implications.

In an academic point of view, the results confirm most conclusions mentioned in the literature on this topic. However, several differences with previous studies have also been found which call for deeper analysis of motivations for and risks of 1/ self-disclosing and 2/ adopting eID systems.

The discussion groups first confirm the importance of risks. Young European people mainly evoked the security and privacy issues and confirm that they fear that someone may use their data without their consent. Other top perceived concerns refer to 1/ the risk that the data could be accessed by people other than those who are authorised to do so and 2/ identity theft, which is particularly important when speaking about online commerce and online banking. As a result, young people are waiting for better control and particularly ask for more information concerning who uses their data and to what extent. However, the results also confirm the importance of privacy paradox: consumers at the same time declare that they value they privacy and do not seem to actively incorporate privacy concerns in their behaviour (Awad & Krishnan 2006).

A significant contribution of this study that is not deeply discussed in the literature deals with the different sources of trust, whether public (offered by the regulation), private (associated with the company offering the service), from peers (i.e. WOM: word of mouth) or linked to the technology itself (Internet and the eID systems). However, most previous work only/mainly focuses on one source of trust, mostly private or public ones (e.g. Backhouse and Halperin 2005). These outcomes therefore offer some opportunity to complete the literature by adding to existing models different kinds of trust sources and different kinds of perceived risks. It will then help to identify the relative importance of those risks and trust enablers in affecting the intent to self-disclose online and to adopt identification technologies.

Finally, the results confirm and complement the conclusion of the literature concerning cultural specificities. Although attitudes are quite similar on some topics (e.g. identity, eID systems and regulation) through the four countries surveyed, young people have specific perceptions depending on the European country where they live. One reason is that although there are countries from the same geographical area and with the same data protection law (Directive 95/46/CE, for the protection of personal data), they don't have the same level of Internet and eID technologies penetration.

For practitioners, our results show a general non knowledge concerning existing eID systems and a doubt concerning the capability of institutions to manage those systems and to offer adequate protection against security and privacy breaches.

However, more knowledge of and familiarity with those new electronic identification systems – through communication/adverts and tests - may build up credibility and acceptance that could be used as a stepping stone to enhance trust in these technologies and thus facilitate their adoption and diffusion. Incentives and clear advantages must be proposed and advertised in order to accelerate the development of trust. The technology itself can also enhance trust by offering users real control over the use of their identity and their personal data. The attribution of labels may as well contribute to building a climate of trust by providing guarantees to end-users.

For policy makers, the results both show a clear benefit to act and some difficulties to overcome.

Our study first confirms that the young European people are quite unaware of existing laws on data protection and of the rights these laws give. This point should be addressed if those new eID systems are to be implemented with success. Hence, whereas those laws exist, policy makers should inform the public about their existence and integrate this information into the education process.

The second obstacle is linked with government untrustworthiness. People want to be safe, but they are wary of governments. Young people do not trust governments but expect them to act.

The third issue deals with gaps and divides in the European population (and even in the youth category itself), whether at the cultural and digital levels. As digital culture and behavioural attitudes vary across EU member states, global policies are not always sustainable although highly desirable (Compano and Lusoli 2009). There is for example a difference between Spain and Germany in the perceived ability of public organisations to manage identification technologies and in the need for repressive laws. These results suggest that eID implementation must be very specific to each country or regional areas.

5.2 Limitations

The first limiting factor of this study deals with the sample which is only composed of young people. Although they are the future web users, they constitute a specific part of the population particularly Internet minded. A broader view of all the populations around the world with different cultural, regulatory and IT backgrounds (diverse nationalities, all ages and both highly skilled and lesser skilled) would be highly desirable although difficult to obtain.

The second limiting factor of this study is linked with the - qualitative - method chosen which is mainly focused on motivations, risks and needs and don't really permit to see the links between all the interesting variables. Additionally, the results are not really "generalisable" as the population interviewed remains relatively small in comparison with quantitative surveys.

5.3 Future work

There is consequently a need to understand more deeply people's perceptions and real behaviours in order to identify ways to enhance the implementation and adoption of such identification systems. Further investigation is required to identify value-added services that may improve and facilitate daily life, at a minimum cost.

This will be done in 2 ways.

Firstly, a second qualitative study with 7 EU27 countries from different regional blocks will be run to better understand Europeans practices, attitudes and policy preferences as regards personal data identity disclosure, with a view of directly assisting policy formulation and consensus in this area.

Secondly, a final questionnaire for a EU27 survey on this topic is being processed that has already been tested in 4 EU countries (Lusoli and Miltgen 2009) and should be conducted later in the year.

6. References

Akman, I. & Mishra A. (2010). 'Gender, age and income differences in internet usage among employees in organizations' in *Computers in Human Behavior* 26, 3, pp. 482-490.

Almeida, J.A.S., Pais A.A.C.C., & Formosinho S.J. (2009). 'Science indicators and science patterns in Europe' in *Journal of Informetrics* 3, 2, pp. 134-142.

Asaro, Peter M. (2000). 'Transforming society by transforming technology: the science and politics of participatory design' in *Accounting, Management and Information Technologies* 10, 4, pp. 257-290.

Awad, N.F., & Krishnan M.S. (2006). 'The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization' in *MIS Quarterly: Management Information Systems* 30, 1, pp. 13-28.

Backhouse, J., & Halperin, R. (2007). A Survey on Citizen's trust in ID systems and authorities. *Fidis Journal, 1* (Online). Available from http://journal.fidis.net/fileadmin/journal/issues/2007/SurveyonCitizensTrust.pdf

Compañó R. & Lusoli W. (2009), The Policy Maker's Anguish: regulating personal data behaviour between paradoxes and dilemmas, Workshop on the Economics of Information Security (WEIS 2009), London, 24-25 June 2009

Eisenhardt, K.M. (1989), Building Theory from Case Study Research. Academy of Management Review, 14(4), 532-550.

Eysenck, M. W. (1974). 'Age differences in incidental learning' in *Developmental Psychology* 10, 6, pp. 936-941.

Fogel, J., & Nehmad E. (2009). 'Internet social network communities: Risk taking, trust, and privacy concerns' in *Computers in Human Behavior* 25, 1, pp.153-160.

Fountain, J. E. (2000). 'Constructing the information society: women, information technology, and design' in *Technology in Society* 22, 1, pp. 45-62.

Gauzente C. & Peyrat-Guillard D. (2007). *Analyse statistique de données textuelles en Sciences de Gestion - Concepts, Méthodes et Applications*, Editions EMS, Coll. Questions de Société.

Gelula, M. H. (1997). 'Clinical discussion sessions and small groups' in *Surgical Neurology* 47, 4, pp. 399-402.

Grijpink, J. (2002). 'Personal number management and identity fraud -- number strategies for security and privacy in an information society' in *Computer Law & Security Report* 18, 5, pp. 327-332.

Gross, R., & Acquisti, A. (2005). *Information Revelation and Privacy in Online Social Networks.* Privacy in the electronic society Conference, Alexandria, VA. Available from <http://www. heinz.cmu .edu/~acquisti/papers/privacy-facebook-gross-acquisti.pdf>.

Hoadley, C. M., H. Xu, J. J. Lee, & M. B. Rosson (2010). 'Privacy as information access and illusory control: The case of the Facebook News Feed privacy outcry' in *Electronic Commerce Research and Applications* 9, 1, pp. 50-60.

Hulicka, I. M., & R. L. Weiss (1965). 'Age differences in retention as a function of learning' in *Journal of Consulting Psychology* 29, 2, pp. 125-129.

Hyder, S. (2005) 'The information society: Measurements biased by capitalism and its intent to control-dependent societies - a critical perspective' in *The International Information & Library Review* 37, 1, pp. 25-27.

Jensen, C., C. Potts, & C. Jensen (2005). 'Privacy practices of Internet users: Self-reports versus observed behavior' in *International Journal of Human-Computer Studies,* 63, 1-2, pp. 203-227.

Jung, I. (2009). 'Ethical judgments and behaviors: Applying a multidimensional ethics scale to measuring ICT ethics of college students' in *Computers & Education* 53, 3, pp. 940-949.

Kim, H-J. (1995). 'Biometrics, is it a viable proposition for identity authentication and access control?' in *Computers & Security* 14, 3, pp. 205-214.

Lago, P. P., M. G. Beruvides, J-Y Jian, A. M. Canto, A. Sandoval, & R. Taraban (2007). 'Structuring group decision making in a web-based environment by using the nominal group technique' in *Computers & Industrial Engineering* 52, 2, pp. 277-295.

Lebart*, L. & A* Salem (1988). *Analyse statistique des données textuelles. Questions ouvertes et lexicométrie*. Paris, Dunod.

Lusoli, W., & Miltgen, C. (2009). *Young People and Emerging Digital Services. An Exploratory Survey on Motivations, Perceptions and Acceptance of Risks* (JRC Scientific and Technical Reports EUR 23765 EN). W. Lusoli, R. Compañó & I. Maghiros (Eds.) Sevilla: EC JRC IPTS. Retrieved 26 April 2010, Available from http://ipts.jrc.ec.europa.eu/publications/

Magkos, E., M. Maragoudakis, V. Chrissikopoulos, & S. Gritzalis (2009). 'Accurate and large-scale privacy-preserving data mining using the election paradigm' in *Data & Knowledge Engineering* 68, 11, pp. 1224-1236.

Mason, J. (1996) Qualitative Researching. London: Sage

Mezgár, I. (2003). 'Role of trust in networked production systems' in *Annual Reviews in Control* 27, 2, pp. 247-254.

Meziane, H., & S. Benbernou (2010).'A dynamic privacy model for web services' in *Computer Standards & Interfaces,* In Press, retrieved 26 April 2010, from http://www.sciencedirect.com/science/article/B6TYV-4YHP00V-1/2/7057d25bf4f588e4f1791fc54c5e5a70

Nach, H., & A. Lejeune (2010). 'Coping with information technology challenges to identity: A theoretical framework' in *Computers in Human Behavior,* In Press, retrieved 26 April 2010 from http://www.sciencedirect.com/science/article/B6VDC-4YBMT85-2/2/7612f853fece8ae253912ec0daa05e0c.

Nau, Douglas S. (1995). Mixing Methodologies: Can Bimodal Research be a Viable Post-positivist Tool? The Qualitative Report, 2(3), http://www.nova.edu/ssss/QR/QR2-3/nau.html.

Nielsen, J. (1993), Chapter 6: Usability testing. In Usability Engineering, p165-205, Academic Press

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. *Journal of Consumer Affairs, 41*(1), 100-126.

Oomen, I. & Leenes, R. (2007). *Privacy Risk Perceptions and Privacy Protection Strategies.* Policies and Research in Identity Management: First Working Conference on Policies and Research in Identity Management (Idman'07), Rsm Erasmus University, Rotterdam, the Netherlands, October 11-12, 2007. Available from <http://www.springerlink.com/content/m047306774615186/>.

Paine, C., U-D. Reips, S. Stieger, A. Joinson, & T. Buchanan (2007).'Internet users' perceptions of privacy concerns' and privacy actions'. in *International Journal of Human-Computer Studies* 65, 6, pp. 526-536.

Ratha, N. K., J. H. Connell, & R. M. Bolle (2001). 'Enhancing security and privacy in biometrics-based authentication systems' in *IBM Systems Journal,* 40, 3, pp. 614-634.

Reinert M (1986), Un logiciel d'analyse lexicale, Les cahiers de l'analyse de données, 4, Dunod.

Ricci, A. (1998) 'Towards a systematic study of Internet-based political and social communication in Europe' in *Telematics and Informatics* 15, 3, pp. 135-161.

Semeonoff, B. (1952). 'On the reliability of the leaderless group discussion technique' in *Psychological Bulletin* 49, 5, pp. 540-541.

Senicar, V., B. Jerman-Blazic, & T. Klobucar (2003), 'Privacy-Enhancing Technologies - approaches and development' in *Computer Standards & Interfaces* 25, 2, pp. 147-158.

Tashakkori, A. and Teddlie, C. (1998). Mixed Methodology – Combining Qualitative and Quantitative Approaches. Applied Social Research Methods Series, Volume 46. Thousand Oaks: Sage.

Wang, H., H. Zhang, C.-Y. Chang, & H-C Chao (2010). 'A universal access control method based on host identifiers for Future Internet' in *Computers & Mathematics with Applications,* In Press, retrieved 26 April 20101 from http://www.sciencedirect.com/science/article/B6TYJ-4Y5H637-6/2/ee24ef1bc00f13ceeb9db30df39494a1.

Wang, S. X. & Taratorin, A. M. (1999).'Alternative information storage technologies' in *Magnetic Information Storage Technology*, 495-530. San Diego: Academic Press.

Ward, P., & C. L Smith (2002). 'The Development of Access Control Policies for Information Technology Systems' in *Computers & Security* 21, 4, pp. 356-371.

Yin R. (1989), Case studies research: design and methods, Sage Publications, Newbury Park, CA

Les autres documents de travail du GRANEM accessibles sur le site Web du laboratoire à l'adresse suivante : (http://ead.univ-angers.fr/~granem08/spip.php?rubrique36) :

Numéro	Titre	Auteur(s)	Discipline	Date
2008-01-001	The Cognitive consistency, the endowment effect and the preference reversal phenomenon	Serge Blondel, Louis Lévy-Garboua	Théorie du Risque	octobre 2008
2008-02-002	Volatility transmission and volatility impulse response functions in European electricity forward markets	Yannick Le Pen, Benoît Sévi	Econométrie Appliquée	octobre 2008
2008-03-003	Anomalies et paradoxes dans le cas des choix alimentaires : et si les carottes n'étaient pas oranges ?	Serge Blondel, Christophe Daniel, Mahsa Javaheri	Economie Expérimentale	octobre 2008
2008-04-004	The effects of spatial spillovers on the provision of urban environmental amenities	Johanna Choumert, Walid Oueslati, Julien Salanié	Economie du Paysage	octobre 2008
2008-05-005	Why do rational people vote in large elections with costs to vote?	Serge Blondel, Louis Lévy-Garboua	Théorie du Risque	novembre 2008
2008-06-006	Salaires, conditions et satisfaction au travail	Christophe Daniel	Economie du Travail	novembre 2008
2008-07-007	Construction communicationnelle du stock de connaissances de la compétence collective – Contribution à partir d'une conversation.	Nicolas Arnaud	Gestion des Ressources Humaines	décembre 2008
2008-08-008	On the non-convergence of energy intensities: evidence from a pair-wise econometric approach	Yannick Le Pen, Benoît Sévi	Econométrie Appliquée	décembre 2008
2008-09-009	Production of Business Ethics	Guido Hülsmann	Economie Politique	décembre 2008
2008-10-010	Time preference and investment expenditure	Guido Hülsmann	Economie Politique	décembre 2008
2008-11-011	Le marché de la photographie contemporaine est-il soluble dans celui de l'art contemporain ?	Dominique Sagot-Duvauroux	Economie de la Culture	décembre 2008
2008-12-012	The newsvendor problem under multiplicative background risk	Benoît Sévi	Microéconomie de l'Incertain	décembre 2008
2009-01-013	Complémentarité de la collaboration électronique et de l'investissement relationnel : étude de cas exploratoire d'un SIIO dans le secteur du meuble	Redouane Elamrani, Nicolas Arnaud	Organisation	avril 2009
2009-02-014	On the realized volatility of the ECX CO2 emissions 2008 futures contract: distribution, dynamics and forecasting	Julien Chevallier, Benoît Sévi	Finance	mai 2009
2009-03-015	The communicational making of a relation-specific skill: contributions based on the analysis of a conversation to strategy-as-practice and resource-based view perspectives	Nicolas Arnaud	Stratégie	juin 2009
2009-04-016	Le droit d'auteur, incitation à la création ou frein à la diffusion ? Une analyse empirique du cas de la création télévisuelle	Françoise Benhamou, Stéphanie Peltier	Economie de la Culture	septembre 2009
2009-05-017	Diversity analysis in cultural economics: theoretical and empirical considerations	Françoise Benhamou, Renato G. Flôres Jr., Stéphanie Peltier	Economie de la Culture	septembre 2009
2009-06-18	L'épargne retraite en entreprise : un état des lieux au regard de l'expérience américaine	Fabrice Pansard, Bruno Séjourné	Finance	septembre 2009
2009-07-19	Options introduction and volatility in the EU ETS	Julien Chevallier, Yannick Le Pen, Benoît Sévi	Econométrie Appliquée	septembre 2009
2009-08-20	Modeling strategic interactions between firms and local authorities – The case of a biotechnology cluster	Alain Berro, Isabelle Leroux	Economie des réseaux	septembre 2009
2009-09-21	The strategy adopted by non-profit care services organizations in dealing with the new French regulatory system: strategic coalitions and reterritorialisation of activities	Isabelle Leroux, Laurent Pujol, Eric Rigamonti	Economie Sociale	novembre 2009
2009-10-22	Une nouvelle lecture du territoire par la limite	Jean-Claude Taddei	Territoire	novembre 2009
2010-01-23	Adoption of new identity-based services: Proposition of a conceptual model based on TAM, DOI and perceived risks	Caroline Lancelot Miltgen	e-marketing	juillet 2010
2010-02-24	Young Europeans' motivations, perceived risks and requirements regarding electronic identification : Some comparative results from focus groups in four EU27 countries	Caroline Lancelot Miltgen	e-marketing	décembre 2010