OBTAINING CONSENT: CONTRIBUTIONS OF THE CONSENT CASE TO DATA SHARING IN SMART CITIES

Abstract:
The objective of this research is to present the way in which consent could be implemented by smart cities concerning the sharing of data of fellow citizens. Based on an exploratory qualitative study carried out among 30 citizens, the results show the importance of the trust placed by citizens in their local authority and emphasize the demands to be met in order to obtain the consent of the inhabitants. These requests are both technical, with the mention of the duration of use of the data, the possibility of the right of withdrawal, the confidentiality of anonymity, and symbolic order with commitments on non-commercial purposes. and on collective social utility. It therefore appears that beyond regulatory and managerial injunctions, a moral injunction also applies to citizens. Consent in smart cities therefore involves regulatory, managerial and moral issues

Keywords:
“ consent ” ; “ smart cities ” ; “ citizens ” ; “ guarantees ” ; “ regulatory ” ; “ moral commitment”

Résumé :
L'objectif de cette recherche est de présenter la manière dont le consentement pourrait être mis en œuvre par une *smart cities* concernant le partage de données des concitoyens. À partir d’une étude qualitative exploratoire menée auprès de 30 citoyens, les résultats montrent l’importance de la confiance accordée par les citoyens à leur collectivité territoriale et insistent sur les demandes à satisfaire pour obtenir le consentement des habitants. Ces demandes sont tant d’ordre technique, avec la mention de la durée d’utilisation des données, de la possibilité du droit de retrait, de la confidentialité de l’anonymat, que d’ordre symbolique avec des engagements sur les finalités non commerciales et sur l’utilité sociale collective. Il apparaît donc qu’au-delà des injonctions réglementaires et managériales, s’applique également une injonction d’ordre moral vis-à-vis des citoyens. Le consentement dans la *smart cities* implique donc le réglementaire, le managérial et le moral.

Mots-clés :
« consentement », « *smart cities* », « citoyens », « garanties », « réglementaire », « engagement moral »

OBTAINING CONSENT: CONTRIBUTIONS OF THE CONSENT CASE TO DATA SHARING IN SMART CITIES

INTRODUCTION

New technologies have led to new uses that bring with them new challenges in terms of security and privacy. From the consumer's point of view, new technologies are being adopted and embraced because of the benefits they bring (Iannone, 2009). No more printing constraints, it is now possible to use a mobile phone to present a ticket and make payments. A simple signature on a PDF can complete a transaction. A simple click on the link received allows you to participate in a conference. All these experiences make the consumer's daily life simpler and easier (Manoury and Burrini, 2001).

However, although they are obvious sources of advantages and consumer benefits, with innovative and personalised services, the new technologies entail major risks in terms of respect for privacy of which consumers are not always aware. From data left behind, voluntarily or not, it is possible to infer sensitive and personal data such as the individual's home, activities, social circle, even health problems, political opinions and religious beliefs (Zang & Bolot, 2011; Jedrzejczyk and al., 2009; Narayanan & Shmatikov, 2009).

In the context of digital offerings, consent implies an agreement on the use of data between those who are affected by the collections and those who collect and process the information. Thus, in order to define new services useful to all inhabitants, local authorities must have data on their citizens. It is therefore necessary to receive their consent to process their data for the purposes of new services for citizens. In these smart city situations, obtaining consent allows the user to exercise a right of control over the personal data that is collected. And the request for consent leads the data controller (i.e. "the data holder") to have to legitimize its collection and processing.

This article examines consent in the context of smart cities projects. After recalling the duality of the injunctions that apply, one regulatory and valid for all organizations, the other more focused on the managerial ambitions of the smart city, we present the methodology of the exploratory qualitative study conducted. It focuses on the opinions and statements of 30 citizens of a metropolis involved in a smart city project supported by Europe. The results summarize the opinions of the citizens when it comes to giving their consent to the sharing and processing of their data. The discussion is an opportunity to underline the importance of trust in the local authority and its competences, and to relate the different requests of the inhabitants to be satisfied to obtain their consent. These requests are both technical, with the mention of the duration of use of the data, the possibility of the right of withdrawal, the confidentiality of anonymity, and symbolic, with commitments on non-commercial purposes and on the collective social utility. It therefore appears that, in addition to regulatory and managerial injunctions, a moral injunction also applies to citizens. Consent in smart cities therefore involves the regulatory, the managerial and the moral.

1. Literature review: consent subject to a duality of injunctions

The vast majority of digital services and products are based on business models that value the personal data of their users (Cecere and Rochelandet, 2012). In order to be able to build the knowledge that marketers and digital project managers need, it is essential to obtain the consent of users of offers and services to the collection and processing of their data, whether it be browsing data or consumption data. As consent is the key to the relationship between users of services and products and the providers

of those services and products, it is essential to obtain it. However, regulatory constraints have increased since the implementation of the GDPR. Therefore, as a prerequisite to any processing ambitions, the first obligation is to obtain users' consent by following the legislator's requirements (Pichonnaz, 2019). The regulatory injunction is now a prerequisite for managerial projects.

The regulatory injunction

The regulatory injunction refers to the requirements of the legislator. For the latter, the expression of consent is a fundamental element of legitimacy for the processing of personal data. It must be given "expressly" for French law, unmistakably for Directive 95/46/EC, and "univocally" for the RGPD, a regulation valid throughout Europe and applied since May 2018.

Most often, the expression of consent goes through the general terms of use (GTU) that the user accepts or refuses. They are usually presented in the form of a long text that explains the different types of data collected, the possible processing and the partners with whom the data may be shared. The text also details the other rights and responsibilities of the different parties involved in the "contractualization". When reading the TOS, the user is supposed to make an informed and explicit choice by checking a box (accept or refuse) with the consequences we know. If the acceptance of the TOS allows access to the service/product, the refusal of the TOS, almost systematically leads to the impossibility of access to the service/product. From then on, consent generally appears as a coercive element with this obligation of acceptance for the consumer in a hurry and focused on obtaining a service (getting information, consulting a site, watching a video, ...). This situation leads researchers to question the freedom of the user. Indeed, is the user really free? Is this form of consent really legitimate?

Seeking to answer the question of the legitimacy of this form of consent, which is ultimately imposed on the user, if he absolutely wishes to have access to this service, researchers conclude that this consent is a coercive element. On the one hand, it is not technically possible to read in detail all the information about the content of the consent to which the consumer commits. It would take 25 full days (24H/24) of reading privacy rules each year to fully go through the TOS of the average number of sites we use (1400 sites) that are presented to him (McDonald and Cranor, 2008; Reidenberg, et al, 2015). On the other hand, the language used and the wording of the consent request is not very understandable by consumers. For example, only 11% of users understand the implications of the cookies they are accepting (McDonald and Cranor, 2010). Finally, consumers are not always able to make decisions that are in their own best interest (Kahneman and Thaler, 2006).

The managerial requirements and ambitions of smart-cities projects

A territorial platform for sharing and reusing data aims to carry out new projects of general interest. In a logic of smart cities, the aim is to develop more efficient and more personalized services for the inhabitants of the local authority concerned.

This type of territorial platform brings together four types of actors. Firstly, the data holders, through their activity, collect or generate data (some of which are personal data on the inhabitants or citizens who use their services). In the second place, the project leaders, who reuse the producers' data to develop services, studies or research. In the third place, the inhabitants or citizens, who act on their personal data collected and stored by the data holders, and participate in studies or use services set up by the project holders. In the 4th place, the platform whose mission is to be the interface allowing and encouraging this sharing and reuse in compliance with the regulations, in compliance with the expectations of citizens, in the interest of the socio-economic development of the territory (support for innovation, new projects, activities...).

This type of platform must offer 3 types of functionalities. The first functionality consists in storing and centralizing the consents collected by the data holders. These consents are collected in the form of "yes", "yes except", "no except", "no" in connection with choices of themes. For example, a citizen chooses "yes I agree to the reuse of my data for development projects EXCEPT" for the themes of "Mobility" and "Education". Conversely, another citizen chooses "no, I refuse the reuse of my data for development projects EXCEPT" for the themes of "Ecology" and "Education". Finally, a last citizen can systematically refuse to share his data: "no, I refuse the reuse of my data for development

projects". This assumes that data holders adopt the thematic typology proposed by the platform for future consents and update the consents already held.
The second functionality consists in allowing residents to: 1) Consult their consents (have a summary); 2) Authorize or revoke a consent; 3) Evolve in the levels of consents by themes (go from "yes/yes except, no except, no); 4) Specify their consent in front of projects in the cases "yes except") and "no except" (for example: a citizen must be able to validate his consent on a project related to the theme "Ecology" on which he had signaled his consent in principle. Does he give his consent to the project "Study of the management of green waste production weight 2022-2023"?); 5) Visualize the projects on which their data are reused (e.g.: a citizen can see on the platform his participation history and his current participations. He can see that he has participated in the project "Study of the management of the production weight of green waste 2022-2023" and that his data contribute to the work of the project "Frequentation of public transport and use of electric bicycles in the Metropolis - winter 2025" and the project "Study of the links between frequentation of Green Spaces and Air Quality")
The third functionality consists in informing the data holders about the data extractions they have to provide to the project owners and in informing the project owners about the volumes of inhabitants/citizens who have given their consent to the use of the data for the benefit of their projects.

2. Methods and results

Methods

The methodology used is based on an exploratory qualitative study. It focuses on the opinions and statements of 30 citizens of a metropolis involved in a smart cities project, supported by Europe.
All individual interviews were transcribed in full before being analyzed for content. This analysis was carried out manually following the classic process of vertical and horizontal analysis. The verbatims that illustrate the results presented here are grouped in Annex 1.

Results

The results presented here summarize the opinions of citizen residents when it comes to giving their consent to the sharing and processing of their data.
This study allows us to understand their perceptions and attitudes, more or less favorable to such a tool, and to know the conditions of their adhesion to this form of platform; this study was thus the occasion to specify what the citizens consider when it is a question of consent.
1°) There is an effect of the proximity of the public representation on the trust granted by the citizen to the local authority.
Consent immediately questions the trust placed in the institution that collects the citizen's data. This trust is all the greater when the local authority is physically close. The citizen has more confidence in the direct level of public representation made by his city than in the higher levels represented by the Region and then the State. The layers of decentralization of state representation lead to differential layers of trust granted by the citizen to the territorial interlocutors who govern him.
However, this trust of the citizen is only valid if it is part of a democratic system of governance. The participants insist that their tendency to trust the community would not be conceivable and effective, even though it is now, if they were to live in a system other than a democracy.
2°) Before consenting to hand over their personal data, citizens want to be informed and reassured about the (non-commercial) purpose of the processing and the future of the data.
The perceived usefulness is a condition *sine quae non* for consenting to the subsequent use of their personal data. This usefulness must be based on the notion of collective interest. Citizens cannot imagine sharing their data if it does not serve to improve the collective and the common good. They insist on this: this data sharing must make sense to them.
Moreover, concerning the non-commercial aspect, as producers of data for the community, citizens hope that their data will never be accessible and used for advertising purposes.

3°) The consent to deliver one's personal data must be based on a personal choice and a voluntary approach of the citizen.
When citizens project themselves in the use of the platform, they agree to share their data according to the principles of citizen engagement.
Indeed, sharing their data would be a way to act in favor of the local community and they would do it as if they were engaging in an associative or humanitarian action. In this respect, it is important that they do it on the one hand, because they want to (personal choice) and on the other hand, that they can feel proactive (voluntary approach).
4°) In addition to the guarantees of anonymity and confidentiality linked to their shared personal data, citizens demand technical control of the data from the community.
Insofar as data management is not the original core competence of the local authority, they question the existence of technical skills. In particular, they question the know-how currently possessed. They may, for some, be dubious about the capacity of the local authority to take on the subject of data.
5°) Consent must be limited to a given period and the right to withdraw must be exercised
The citizen considers that consent can be questioned at any time. Consent must be regularly questioned and requested again. It is then subject to confirmation by the citizen who can then choose to withdraw his consent and stop accompanying a project. This suggests flexibility on the part of the local authority in the face of the right granted to the citizen to change his mind.
In these requests for continued consent, the citizen imagines the possibility of "updating" his data.
When the citizen chooses to withdraw his consent, he also wishes to be able to exercise a right of control over his data, or even to exercise a total withdrawal (with or without the purpose of portability). Through this possibility of control, the proposed consent would express the principle of "data sovereignty".
6°) Consent is dependent on the perceived privacy of the data.
Citizens feel that not all data has the same level of publicity.
Some data such as marital status, housing, seem to be more easily deliverable and shareable. These data are almost public information, since anyone can access them by walking down the street, for example, and looking at the mailboxes and observing the housing.
On the other hand, other information is less public. It concerns everything that is related to the activities of the individual and the people he or she lives with. These are, for example, activities related to leisure and travel. The participants feel that they are less inclined to disclose this information because it concerns the protection of privacy and the protection of those around them. In this regard, the special case of health data should be noted. It seems to be the only one that can be shared and exported from the local territory. Indeed, citizens declare their consent to communicate their health data on the condition that they know how the data will be used and processed. Their consent is also conditional on the idea of serving public research and the common good in terms of health.
7°) Graduated consent according to the nature of the data produced or transmitted by the citizen.
There is a graduated vision of the collection and current uses of their personal data which is at three levels as follows.
- There is data that the community obtains de facto since the citizen has delivered information voluntarily to have services from the municipality and be identified as a rightful claimant of this municipality.
This de facto obtained data would not require consent since it is already freely provided. It is therefore data for which consent is obvious. This would be referred to as "open access" to the data. The consent to share this data is then almost systematically acquired ("yes" consent).

There are some data that the community can (or could) obtain through a request for access to files. This would involve requesting information on their clients and beneficiaries from the structures offering services managed by the public sector (traffic, transport, water, etc.). This information can be direct, since it is available and accessible in the files of the structures providing these services. It can also be indirect information because it is obtained by successive cross-checking of personal data from different files (services offered by the town hall + services offered by the local authority).

E.g.: space for the pool

- The citizen is therefore aware that processing and cross-checking can be established by the entity. Insofar as the community can have access to these data, which are relative, in a broad vision, to the different services offered by the city, we will then speak of a "tacit access" to the data. Consent to the sharing of this data is then normally given if the citizen does not wish it, he or she will express it (consent of the "yes, except" type).

E.g.: data on water consumption/opening of meters, mobility data (geolocation).

- Finally, there is the data retrieved by search engines and private companies (restaurants, stores...) with which the citizen interacts as a consumer. These data allow to identify the tastes and preferences of individuals.

They believe that this data belongs to the private sphere and therefore the community has no legitimacy to use it. In this case, there is a refusal of consent to the collection of data that could be described as "zero consent" to access the data. Consent to the sharing of this data is normally refused ("no consent"). If the citizen wishes to share, however, he or she will express it ("no, except" consent).

E.g.: data on cultural space, leisure, consumption

3. Discussion and conclusion

Most of the work on consent to provide personal data relates to situations where it is a question of obtaining access to a service via an application or a fixed or mobile Internet site.

In the more specific and recent case of digital platforms proposed by local authorities, consent questions 1) the link between trust and proximity of the territorial actor, 2) the notion of a citizen's commitment in the act of sharing, 3) the question of the collective perceived usefulness of projects, and 4) the technical skills of the platform's owner and manager. The understanding of these aspects guides the choices regarding the envisaged characteristics of this consent.

As we have seen, the moral injunction towards the citizen implies a consent to the sharing and reuse of data in the framework of smart cities, which are technical, with the mention of the duration of the use of the data, the possibility of the right of withdrawal, the confidentiality of anonymity, and symbolic, with commitments on the non-commercial purposes as well as on the collective social utility.

Our research thus shows that a moral injunction towards citizens is added to the regulatory and managerial injunctions in the context of smart cities projects.

References

NARAYANAN A. and SHMATIKOV S. (2009), De-anonymizing social networks. In *Proceedings of the 2009 30th IEEE Symposium on Security and Privacy*, SP ’09, pages 173–187, Washington, DC, USA, IEEE Computer Society. URL : http://dx.doi.org/10.1109/SP.2009.22, doi:10.1109/SP.2009.22.

ZANG H. and BOLOT J. (2011), Anonymization of location data does not work : A large-scale measurement study. In *Proceedings of the 17th Annual International Conference on Mobile Computing and Networking*, MobiCom ’11, pages 145–156, New York, NY, USA, 2011. ACM. URL : http://doi.acm.org/10.1145/2030613.2030630, doi:10.1145/2030613.2030630.

Kahneman, D., et Thaler, R. H. (2006). Anomalies: Utility maximization and experienced utility. Journal of economic perspectives, 20(1), 221-234.
JEDRZEJCZYK L., PRICE B., BANDARA A., and NUSEIBEH B. (2009), I know what you did last summer : risks of location data leakage in mobile and social computing. 01.
McDonald, A. M., et Cranor, L. F. (2008), The cost of reading privacy policies. *Isjlp*, *4*, 543.
McDonald, A., et Cranor, L. F. (2010), Beliefs and behaviors: Internet users' understanding of behavioral advertising. Tprc.
Reidenberg, J. R., Breaux, T., Cranor, L. F., French, B., Grannis, A., Graves, J. T., Ramanath, R. (2015), Disagreeable privacy policies: Mismatches between meaning and users' understanding. Berkeley Tech. LJ, 30, 39.
doi.acm.org/10.1145/2030613.2030630, doi:10.1145/2030613.2030630.

Appendix 1- Table of verbatims

Résultat	Verbatim
There is an effect of the proximity of public representation on the confidence of the citizen in the local authority	*"Yes, more confidence because it is a community" (C15)* *"Again, by a public person" (C10)* *"I find it normal that the city has this data but not that it uses it without consent" (C2)* *"I would have confidence because it is a community, but after all it depends on who is in charge of the community, on certain political representations, I would have doubts... I wouldn't have confidence in all the political groups. At some point, there could be abuses" (C14)*
Before agreeing to give up their personal data, citizens want to be informed and reassured about the (non-commercial) purpose of the processing and the future of the data	*"You need to be informed and know why... There need to be guarantees that the data is not used for any other purpose than investigation" (C18)* *"I don't want to be in fear of commercial use" (C3)* *"The problem is that our data is sold and resold by private companies .... There is a moment when we are saturated with information because everyone has access to our information, even on things we did not ask for" (C22)* *"It has to have something to contribute as a citizen" (C19)* *"If personal data is used for the collective, for improvement, it makes sense" (C14)* *"I am ready to give information if it is for example for a medical investigation or for public research, then I am ready to give information. If it is a request from a private company, I would be much more reticent" (C4)*
Consent to provide personal data must be based on a personal choice and a voluntary approach by the citizen	*"It's for the community, so the benefit is there, we have to get something positive out of it. It's going to be positive for the community, so it doesn't need to be positive for us personally" (C22)* *"At the level of governance, if it's done with a view to well-being and doing well, then it would bother me less because we know more or less what a data collector would do, it's "monitorable". In another type of governance, i.e. with other political leaders, we experienced this at the beginning of the century, more authoritarian and well I don't know" (C1)*
Citizens demand guarantees of anonymity and confidentiality of their shared personal data, and technical control of the data by the community	"Anonymity! I am aware of the protection of the system. Doing penetration tests because nowadays there are risks of hacking, all kinds of manipulation are possible. We need cybersecurity" (C19) "Cybersecurity is essential in terms of how it is used, where it is stored, who manages it, who has access to this information, how it is kept and secured to reassure the user" (C9) "I just don't trust the ergonomics of the sites created by the public service" (C13) "Wary of the control, where it is stored, in relation to cybersecurity" (C9) "It is important to have a guarantee that it is anonymous, that it will not leak, that someone will not be able to attack the system, retrieve information, cybersecurity on my data, that it will not be sold to private actors for shopping centres" (C10)

Consent must be limited to a specific period and the right to withdraw must be exercised	"I think it is normal that the city has this data but not that it uses it without consent" (C2) I think it's normal for the city to have this data, but not to use it without consent" (C2) "To have the right to look at it, to withdraw it, possibly if there is data that I think is harmful, I would like to be able to simply remove it" (C5) "I think that it should be possible to disengage, to unsubscribe when you no longer see the interest, the desire. You have to give people freedom because otherwise they will feel a bit obliged, as if their hand is being forced" (C11) "We need total transparency in the purpose of this database, an unconditional right to withdraw, and really drastic computer security so that this data stays where it belongs and does not end up elsewhere" (C5)
Consent is dependent on the perceived privacy of the data	*"I think she has a lot more than I think she does, but I can't say how far it goes" (C3)* *I think she has a lot more than I think, after that I can't say how far it goes" (C3) "Civil status, um, family, ascendants, and well the part about water, water and electricity consumption, if we bought a house" (C7)* *"I imagine that she already has some. All the identity data, civil status data, after that I think she can have access to lifestyle data but I don't know how she gets it back" (C10)* *"She also knows from the council tax and property tax the living space of my house, the size of my garden, so all these elements otherwise I don't know, she certainly doesn't have my health data for example, I hope, because that remains my personal medical file" (C15)* *"Having sovereignty over the data that concerns me, that belongs to me... we must respect our private life, our intimacy has the right to be protected. There are still inalienable data" (C20)*
A graduation of consent according to the nature of the data produced or transmitted by the citizen.	"Anything that could be discriminated against for example communicating a salary, private hobbies, sexual orientation, religious orientation, these are very private things" (C2) "It would bother me that someone in the sense of a human being and that no one knows individually who I am and what I usually do and go out, it would bother me because I would be afraid that it could be misused. It's about the collection of information and its use" (C3) "To have the right to look at it, to withdraw, possibly if certain data that I consider harmful, I would like to be able to simply discard it" (C5)