MASTER IN BUSINESS ENGINEERING PROFESSIONAL FOCUS IN ANALYTICS & DIGITAL BUSINESS

What is the perception of the privacy versus security trade-off of citizens in smart cities
the case of facial recognition

Gévart, Antoine

Award date:
2020

Awarding institution:
University of Namur

What is the perception of the privacy versus security trade-off of citizens in smart cities : the case of facial recognition

Antoine GÉVART

Directeur: Prof. I. Jureta

Mémoire présenté
en vue de l'obtention du titre de
Master 120 en ingénieur de gestion, à finalité spécialisée
en Analytics & Digital Business

ANNEE ACADEMIQUE 2019-2020

Université de Namur, ASBL
Faculté des Sciences économiques, sociales et de gestion – Département des Sciences de gestion

Rempart de la Vierge 8, B-5000 Namur, Belgique, Tel. +32 [0]81 72 48 41/49 58, Fax +32 [0]81 72 48 40

Acknowledgements

As a prelude to this thesis, I would like to thank all the people who played an important role in its completion.

First of all, I would like to thank my thesis promoter, Mr. JURETA, for his support, patience and availability. I would also like to thank him for his judicious advice and his listening skills, which contributed to my reflection and to the successful completion of this work.

Next, I would also like to thank the University of Namur for the quality training it has been able to offer me throughout my academic career. I would therefore like to thank in particular the staff of the University and the teaching staff who have enabled me to acquire a great deal of theoretical knowledge and the open-mindedness that is essential for the completion of a thesis.

I would also like to thank my family who supported and accompanied me from the beginning of my studies until the completion of this thesis. I would particularly like to thank my parents for their trust and encouragement throughout my university career. I will also not forget to thank my friends Alexandre Denis, Gilles Hamidouch, Harold Tellier and Louis Renard for their support as well as their discussions and constructive criticism throughout the realization of this work. Finally, I would like to thank Claude Gévart, my grandfather, for his attentive rereading and the passion he instilled in me in the choice of my studies.

Contents

List of Figures

List of Tables

Abstract

Our world is constantly changing and the impact that new technologies play in this evolution is undeniable today. Many challenges will have to be met and we will have to live with these technological advances on a daily basis. Thus, the concept of Smart City has become more and more important in the last few years and a lot of research has been done on it. In addition, we can also observe a particular attention to the use that is made of data in terms of security and privacy.

In the context of this thesis, we have been interested in studying a singular and inherent application of the Smart City, namely facial recognition. This simple study would not be of much interest because many people have already looked at it. However, we found that there was little or no analysis of citizens' opinions on the subject of facial recognition and data. However, citizens are a central part of the Smart City concept and special attention must be paid to them in order to understand their demands and desires. This information has therefore prompted us to articulate the thesis research question under: "What is the perception of the privacy versus security trade-off of citizens in smart cities : the case of facial recognition".

To answer this research question, we first sought, through literature research, to understand the concepts involved. Thus, the first part of this thesis will focus on defining and understanding the very broad concept of Smart City as a whole. The second part of the work will then describe the complexity of data collection in Smart Cities and list the challenges and threats in terms of security and privacy. The third part will aim to link and regroup the first two thanks to the innovative concept of facial recognition.

Finally, in the last part of this thesis and thanks to the theoretical knowledge retained, we will discuss these issues with citizens in order to understand and analyze their position. The main objective of this paper is therefore to propose a look at the citizens' opinion on the topics discussed. Thus, thanks to the theoretical reading proposed in this thesis, the reader will be able to form a global knowledge and an opinion in order to confront himself with the results obtained from other citizens.

Chapter 1

Smart Cities

Our entire society is currently undergoing a transition to a new way of life, with the arrival of ICT technologies at the centre of our attention. This society is also facing many challenges such as climate change, public health issues and the impact of economic crisis.

In addition, we are currently experiencing strong demographic growth and this is also impacting our cities with ever-increasing urbanisation every year. Indeed, it is estimated that by 2050 nearly 85% of the population will live in urban areas [25], which will lead to many challenges in terms of pollution management, mobility and infrastructure [96].

It is in this context of demographic boom, major societal challenges, emergence of new technologies and increased competition between territories and megacities that the concept of Smart City has become popular in recent years. The aim of this smart city is to respond to the challenges we will have to face by delivering a liveable and sustainable city for everyone [30].

This first chapter aims, first of all, to define the concept of Smart City through its various names and definitions. In a second step, we will discover the main components of a Smart City and the requirements to reach that type of city. Finally, some examples of the deployment of smart cities in Belgium and abroad will be presented in order to have a clear vision of how this type of technology can work and be implemented.

1.1 What is a smart city ?

1.1.1 Towards a definition of the smart city

The name Smart City has become more and more popular in recent years all over the world. This concept is perceived by everyone as the possibility to respond to the challenges of the present and the future with innovative technological solutions.

However, although this name is quite familiar to the general public, it is rather difficult to define precisely what a Smart City is. Moreover, the word "smart" is sometimes replaced by "intelligent" or "digital" cities[6]. There is no real consensus on an exact definition of the smart city, despite numerous attempts to do so. The name "Smart City" is in fact a fuzzy concept[24], which sometimes makes it difficult to understand and fuels debates on the precise and adequate establishment of a universal definition[81]. Consequently, there are a number of definitions that are all equally valid, and this section provides a non-exhaustive list of them in order to understand the principle and the issues behind the concept of "Smart Cities".

The first use of the term actually dates back to the 1990s when people were trying to find meaning in the new ICT technologies used in modern urban infrastructure[5]. Since then, many people have sought to define the concept of smart cities precisely by pooling common ideas.

Although initially strongly focused on the technological side, the definition has recently been expanded to include more human and social dimensions as well as promoting an environmentally friendly city. Many terms are common to the different definitions of the smart city but as a starting point, we take the definition brilliantly set out by the Smart City Institute, a spin-off of the University of Liège: "The smart city is an ecosystem of stakeholders (governments, citizens, businesses, NGOs, universities, international institutions) in a given urban territory, engaged in a process of sustainable development, while using technology as a facilitator to achieve these sustainability goals and carry out related actions"[58]. The idea here is to ensure the sustainability and durability of a territory while putting the well-being of citizens at the centre of decisions.

Moreover, authors such as Hollands rightly point out that these digital technologies are the key to developing the social, human sides of a city[53]. In one study, the smart city is seen as an interconnected city by emerging technologies. Through a number of data collection applications discussed in Chapter 2, the smart city collects and analyzes data to optimize and improve the quality of life of citizens within the city[51]. On this point, many authors agree that the city will perform well if its level of digitization is very high.

The use of these technologies must be used in an integrated way by citizens and governments in order to reap the full benefits and solve the various problems that an intelligent city might encounter[67]. It is therefore very clear that the ICT sector is at the centre of the approach and deployment towards a smart city. It is this concept that is at the centre

and will make it possible to manage the challenges of tomorrow due to ever-increasing urbanisation. In their 2013 report, [37] give us some figures on the weight that the technology sector could weigh in the smart city approach and tell us that investments in this direction are already very numerous today: "the share of technology in foreign investments in the world's metropolises is increasing: in 2012, 36% of international investments in Paris were concentrated in the IT (information technology) telecom sector. For several years now, these investments have surpassed all other types of investment in these cities, starting with services and textiles". Although the notion of deploying new technologies is the basis of a smart city, it is worth recalling that this notion is not enough and that the human being remains also a central pawn.

Indeed, the development of smart cities is not simply limited to the massive, pushy arrival of new technologies. The main objective is, above all, to ensure the longevity of the territory while putting the citizens at the centre of the concerns and initiatives carried out. Therefore, ICT technologies must be put to good use in all the sectors that make up the smart city so that these cities are as environmentally friendly as possible. These technologies must work hand in hand and join forces in order to facilitate the exchange of information, thus reducing economic and ecological costs, hence the concept of smart grids as described by[37]: "The city tends to be designed no longer in terms of buildings whose performance is assessed in isolation, but increasingly at the neighbourhood level. Buildings are only truly intelligent and environmentally friendly when they are connected to each other". These smart grids are, therefore, electrical networks that allow the exchange of information between person A and person B in real life, which makes it possible to adjust the flow of information and to use only the electricity necessary for communication, allowing for significant savings and a reduction in the carbon dioxide footprint[100].

Other authors support the importance of human capital in the deployment of smart cities. Thus, according to[25], it is paramount to have humans co-exist with technology and work with citizens to overcome the challenges and problems that the city may encounter. Human capital must be taken into account because citizens are the major actors in a city and contribute to its evolution and living by sharing their knowledge and expertise for the benefit of society. The use of technology alone would make it impossible to set up this kind of city because citizens' expectations can only come from their own will, technologies must be thought out and adapted for and with all segments of the population in order to include everyone in this technological process; "when social and relational issues are not properly taken into account, social polarization may arise as a result. This last issue is also linked to economic, spatial, and cultural polarization"[25]. Thus, by including people in development, the notions of creativity and knowledge have been added to the concept of the smart city. Citizens pool their knowledge, and a city can be said to be smart when culture, education and socialization are improved through the efforts of stakeholders in society[5]. Nam and Pardo[77] add that the city must also be a motor for people to meet each other in order to build relationships and create an intelligent community of committed actors. Citizens are at the heart of the project, and the Smart City plays a role as a facilitator of encounters between these people, as Moreno explicitly states: "a Smart City is not a software but must be a method that aims to make the city a place to live and meet"[32].

Therefore, in addition to having a "Top-Down" strategy, where decisions are made by governments and leaders, the concept of smart cities adds the "Bottom-Up"(Figure 1.1.) side, where decisions and ideas come from the citizens who are at the base of the structure. In the case of smart cities, little is fixed in advance and it is primarily the voice of the citizens that is at the centre of attentions and decisions. The citizens therefore form a united system in order to be able to carry out a sustainable policy that respects everyone's well-being[58].

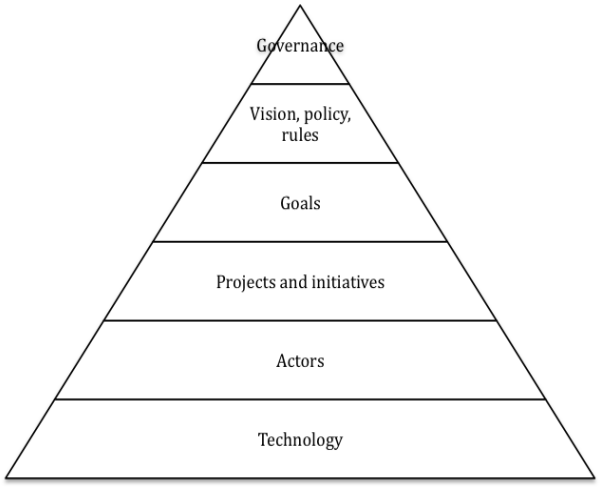


Figure 1.1: Bottom-up smart city development path[36]

Consequently, in the end, all the authors agree that the concept of the smart city includes both the use of ICT technologies on a well-defined territory and with objectives to be achieved. Humans have a predominant place in smart cities through their social interactions and they share a common goal of sustainability of their territory and preservation of the environment. There are many accurate definitions of the "intelligent" city, of which the table below is a non-exhaustive list, but we can also take as a solid basis for the continuation of this work the definition given by [36] in her article : "A smart city is a well defined geographical area, in which high technologies such as ICT, logistic, energy production, and so on, cooperate to create benefits for citizens in terms of well being, inclusion and participation, environmental quality, intelligent development; it is governed by a well defined pool of subjects, able to state the rules and policy for the city government and development".

Definition	Source
"Smart city as a high-tech intensive and advanced city that connects people, information and city elements using new technologies in order to create a sustainable, greener city, competitive and innovative commerce, and an increased life quality."	Bakıcı et al. (2012)
"A city is smart when investments in human and social capital and traditional (transport) and modern (ICT) communication infrastructure fuel sustainable economic growth and a high quality of life, with a wise management of natural resources, through participatory governance."	Caragliu et al. (2011)
"A city combining ICT and Web 2.0 technology with other organizational, design and planning efforts to de- materialize and speed up bureaucratic processes and help to identify new, innovative solutions to city management complexity, in order to improve sustainability and livability."	Toppeta, D. (2010)
"A city "connecting the physical infrastructure, the IT infrastructure, the social infrastructure, and the business infrastructure to leverage the collective intelligence of the city" "	Harrison, C. et al. (2010)
"A smart city is based on intelligent exchanges of information that flow between its many different subsystems. This flow of information is analyzed and translated into citizen and commercial services. The city will act on this information flow to make its wider ecosystem more resource- efficient and sustainable. The information exchange is based on a smart governance operating framework designed to make cities sustainable."	Gartner (2011)
"Smart cities are the result of knowledge-intensive and creative strategies aiming at enhancing the socio-economic, ecological, logistic and competitive performance of cities. Such smart cities are based on a promising mix of human capital (e.g. skilled labor force), infrastructural capital (e.g. high-tech communication facilities), social capital (e.g. intense and open network linkages) and entrepreneurial capital (e.g. creative and risk-taking business activities)."	Kourtit and Nijkamp (2012)
"The application of information and communications technology (ICT) with their effects on human capital/education, social and relational capital, and environmental issues is often indicated by the notion of smart city."	Lombardi et al. (2012)

Table 1.1: Definitions Smart Cities

1.1.2 Main components and framework

After trying to define as best as possible what a Smart City is and who its main actors are, this section focuses on the different dimensions that make up the Smart City. We have seen that thanks to ICT technologies, citizens can coexist together with the ultimate goal of sustainability of their territory. However, this is very complex, indeed the fields of application for ICT are very numerous in a city. By means of real-time data collection and analysis, which will be discussed throughout this work, the intelligent city can be described as a very complete organic system with many interdependencies between its components. The challenges are numerous and various fields of applications are therefore necessary in order to respond as precisely as possible to the challenges facing a smart city. Given the fact that the Smart City is a fuzzy concept[24], there is also no consensus on the number as well as the names of the different dimensions that make up the Smart City. For example, Griffinger[49] sees four main components of a smart city, namely "industry, education, participation and technical infrastructure". However, this classification has since evolved, and many people have sought to find the components of a Smart City. As result, there are many possible domains and sub-domains making the Smart City a very complex framework. For the sake of ease of understanding, it will be question of explaining the 6 dimensions retained by[71] in his work in order to have an uniformity in the terms. These 6 dimensions are also taken up by the Smart City Institute[58] as the main dimensions "encompassing all aspects of a Smart City". These 6 dimensions are, therefore, the following ones:

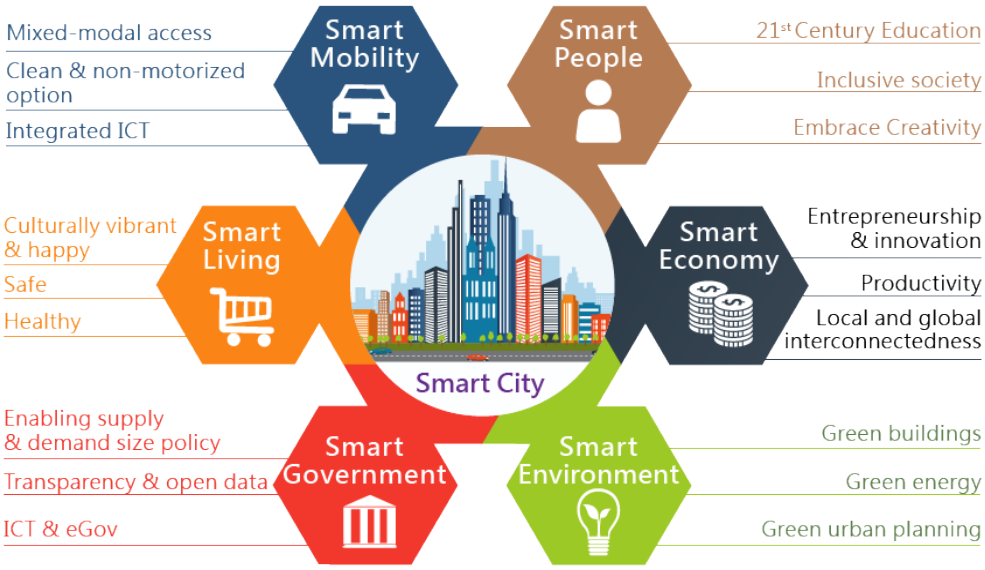


Figure 1.2: Framework Smart City[34]

- **Smart Environment**

The preservation of the environment is at the centre of our concerns nowadays and the Smart City seeks, through the use of ICT, to preserve the sustainability of our territories[58]. A so-called intelligent city has to manage natural resources with great care, as these ones are unfortunately not inexhaustible. This city, which wants to be sustainable, must also take care to limit the emission of polluting gases, including carbon dioxide, which is responsible for disastrous damages to the ozone layer. The smart grids[100], which are management systems using new technologies, therefore allow better management of waste as well as water and air pollution, thus giving the city an opportunity for significant sustainability. Intelligent cities also rely on their own production of so-called "green" and renewable energy in order to be able to deliver it to all its citizens while limiting the impact for our planet. Finally, the multinational Deloitte, in a 2015 report, adds the concept of "Smart Buildings" where new buildings are equipped with thousands of sensors to continuously collect data and adapt the amount of energy to be delivered for the viability of the building without excess of consumption[39].

- **Smart People**

As previously emphasized by[77], the human dimension is one of the pillars of the Smart City. Indeed, all technological and digital efforts are made around the citizens, putting them at the center of the city's attention. The Smart City Institute[58] speaks of an "inclusive society", working hand in hand with the use of technology and aiming to strengthen human and social capital. The notions of multiculturalism, mutual aid and creativity, in particular, are considered essential for a Smart City. The aim here is also to highlight education and foster the talents present in citizens in order to exploit everyone's capacities to the best of their ability. The "Smart Citizen" is therefore the one who promotes tolerance and seeks to improve his or her city through the relationships he or she builds and the challenges he or she takes up.

- **Smart Economy**

Due to the massive arrival of new technologies, it is essential to review economic models because our society is undergoing major changes. The goal of the Smart Economy is to develop a strong economy based on the local and sustainable resources of the city. The development of this strong economy allows smart cities and territories to be competitive with each other and thus to push back their limits. The smart economy also supports business innovation, and this is for many a key to success. This new economy is therefore digital and numerical-based, but it also aims to increase as much as possible the financial capacity and well-being of its citizens. One of the solutions already employed is the circular economy based on the perpetual reuse of waste in order to limit the economic and ecological impact. Thus, according to[58], the Smart Economy "concerns innovative business models that support sustainable economic competitiveness, innovation and interconnections between local and global economic eco-systems".

- **Smart Mobility**

Large cities have a significant number of citizens and people working in them. As a result, all these people travel by car or public transport, which very often causes traffic jams and recurrent mobility problems. The Smart Mobility concept, therefore, aims to manage logistics flows and infrastructures as well as possible in order to solve mobility problems to a considerable extent. This is made possible by providing citizens with digital tools that enable them to find the modes of transport that best meet their expectations. The impact on the environment is once again very important for the smart city, and public transport is therefore favoured, as the Smart City Institute[58] reports: "Smart Mobility includes a modern and sustainable transport system, integrated into a plan that emphasises public transport modes and multimodal options". Mobility can therefore be seen as a service for citizens and helps to solve many problems such as; the reduction of road accidents via intelligent sensors to regulate speed, the decongestion of urban traffic in all types of transport, or parking difficulties in large cities via intelligent applications that allow to visualize vacant spaces in real time.

- **Smart Living**

Large, densely populated cities often face problems of insecurity, housing and public health. It is in this context that the concept of Smart Living comes into play by aiming to improve the well-being, health, access to housing, culture and security of its citizens[40]. Through the use of new technologies, smart cities aim to improve the daily life of its citizens with, for example, the introduction of smart cameras to guarantee greater security in the city, an example that will be discussed in chapter 3 of this work. E-health[8] has also become popular in recent years and aims to make good use of new technologies in healthcare to improve the quality delivered. Therefore, according to the Smart City Institute[58], Smart Living "is concerned with improving the quality of life and safety in the city through the range of services offered, changes in citizens' lifestyles, social cohesion and tourist attractiveness. It also concerns everything relating to e-health, culture, social services and the availability of better quality housing".

- **Smart Governance**

As previously reported via the "Bottum-up" strategy, the idea of Smart Governance is to put the citizen at the centre of attention and to establish collective participation in the decisions of the smart city. The Smart City Institute[58] defines Smart Governance as the dimension that "concerns the services and interactions that link and integrate public, private, civil and European organisations in a more transparent and open decision-making process, through the use of new technologies such as e-services, intelligent data management (especially Big Data Management) and citizen participation". Smart Governance therefore aims to increase citizen participation and to become fully transparent with regard to the collection and use of data. The ultimate goal is to use new technologies as a vector towards a completely new form of governance, e-government.

1.2 Requirements and implementation Smart Cities

In this section, we will see what are the steps to evolve towards the smart city denomination. Indeed, Smart City is a successful process that comes to the end of a long thought by the stakeholders of a city or territory. This section is intended to be a simplification of the approach and requirements necessary to build a smart city. The way in which data are collected and processed using Information Communication Technologies and the resulting challenges will be further explained in chapters 2 and 3. Of course, there is no one single method to achieve smart city design, but for the sake of clarity, we are interested in this work in how the Smart City Institute[58] views the requirements to underpin this ideal of a city that combines technology and citizen well-being. Here are the steps and requirements to be completed in order to successfully implement and complete a Smart City project.

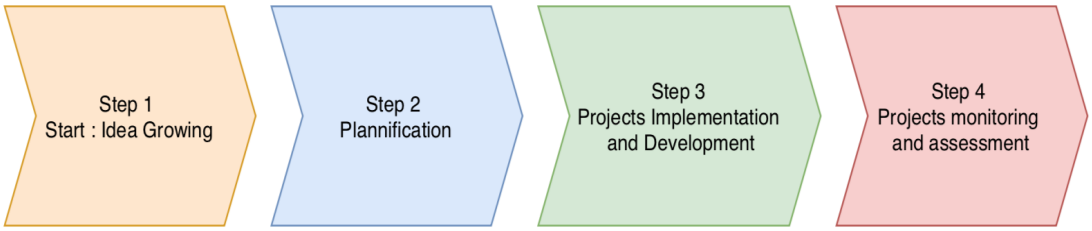


Figure 1.3: Implementation of a Smart City

First of all, the will for a transition to an intelligent city must be present in a city's decision-making authorities. Indeed, these people involved in the politics of their city, are an essential element because they are the only ones who have the power to change things. Nevertheless, as the Smart City Institute[58] reports, some of the will can also come from the private sector or from citizens themselves through the bottom-up system[5], but these will not be sustainable in the long term without the obvious support of policy makers. Secondly, since ICT is a major element of the smart city, one or more people with an attraction for technology must also be found to motivate and justify the transition that needs to be made. According to[58], the leader(s) "are not the only person(s) to act, but rather they are the one(s) who inspire and bring stakeholders together to jointly undertake and maximize efforts to achieve common goals". We have also seen the many domains and sub-domains that make up the Smart City framework and this transition process is also intended to be a multi-sectoral and cross-cutting process. This cross-cutting team will be paramount because it will cover all the areas and challenges that the Smart City comprises. The teams that make up the project's start-up are therefore intended to be united and to have a common goal: the transition towards a sustainable city, concerned about the well-being of its citizens

through the intelligent integration of new technologies. In order to best respond to the challenges of tomorrow, the Smart City must promote cross-sectoral work and integrate the collective participation of citizens[5].

Then, in a second step, it is important to plan projects before implementing them. In order to clearly identify the objectives to be achieved and the projects to be carried out, it is imperative to know the specificities of each territory or city in terms of social, economic and cultural conditions or urban infrastructure. This step is paramount because it will allow, in the long term, to meet the objectives with the resources available at the beginning. Thereafter, it is advisable to carry out benchmarking with other cities similar to ours in order to correctly analyse the opportunities and threats. This analysis will allow our city to avoid reproducing the mistakes made by others and to improve the achievements already made in the past. These objectives and projects to be carried out must therefore be rigorously defined and drawn up by a competent team and must be classified in the different fields of action that make up the Smart City[76]. These projects put on the table must then be rigorously followed up and monitored through measurement and performance indicators. Thus, the European project CityKeys[15] has enabled the implementation of numerous Key Performance Indicators allowing project leaders to continuously measure the proper functioning of their projects. Finally, communication must be a permanent part of the process because it allows transparency regarding the progress of projects and motivates citizens to become individually involved in the projects[58]. This communication can of course be done through all types of channels.

The third step is the most important, as it aims to implement the projects and ideas designed by the stakeholders, it is the culmination of the work done. The implementation of these projects, therefore, responds to needs and objectives previously identified during the planning stage. These projects can, of course, cover several areas and sectors by linking them via ICTs. It is important to carry out the implementation of these projects in order of importance and need.

According to [14], it is essential to form competent and cross-cutting teams to supervise throughout the implementation of projects. Moreover, as seen in point 1.1., the citizen must also be part of the adventure, and a collaborative environment is necessary for things to run smoothly. Prior to implementation, stakeholders must have a good knowledge of new technologies in order to ensure that they are properly integrated into the projects that are started. It is the responsibility of the project leaders to choose scrupulously the type of technology for each project undertaken. Thus, according to[17], the available technologies can be divided into four main families: "Connectivity infrastructure", "Sensors and connected devices", "Integrated operation and control centers" and "Communication interfaces". The concepts of Big Data, Open Data and Internet of Things can also be considered as basic technological elements for Smart Cities and will be explained and clarified in Chapter 2.

However, these projects are expensive, and partnerships and funding are needed to implement them. The sources of financing are varied and numerous, such as funding from governments, private companies willing to invest in their territory, or a fairly recent solution: crowdfunding. These different steps are essential and constitute a solid base and a necessary guarantee to achieve the final objective; the implementation of the project[58].

The last step is to ensure that the projects put in place are running smoothly on an ongoing basis. The monitoring and evaluation of results can be compared on the basis of Key Performance Indicators[15] and, depending on these results, adjustments can be made. Adjustments and modifications are therefore carried out in order to rectify potential deviations and move closer to the initially set objectives. Furthermore, these projects are also evaluated and criticized by the most important parts of the Smart Cities; the citizens. It is through feedback from the experiences of its citizens that a city can best align the challenges of the future with the requirements and well-being of its citizens[17]. An integrative framework for this Smart City initiave can be available below[63].

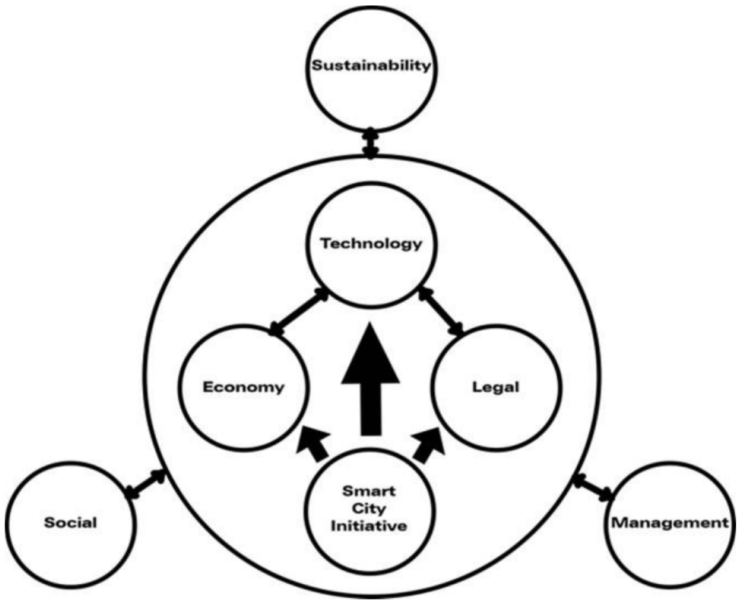


Figure 1.4: Framework Smart Cities initiative[63].

The roadmap for implementing a smart city can be also modeled using a BPMN 2.0 process flow using the Signavio tool[90] available in Appendix A. This flow aims to model the process required to implement smart city projects involving stakeholders and technologies. For the sake of clarity, this process only models the view of Smart Cities, considering people and technologies as black boxes. Smart Cities are modelled here as an actor with a sequence of processes to follow leading to the achievement of a smart city and projects that go in that direction. The "Smart Cities" actor, in accordance with what has been reported in this point 1.2., interacts both with people and technologies.

1.3 Examples of Smart Cities

After having defined and contextualized the concept of Smart Cities, this section aims to relate concrete examples of projects already carried out. Indeed, although it is impossible to have a hundred percent "smart" city, many cities have tried to innovate in Belgium and around the world in order to start the transition to a new way of life. These projects are rooted in each of the 6 dimensions seen above and make it possible to, step by step, make the city evolve towards a more sustainable management of life by integrating ICT in the process.

1.3.1 Progress in Belgium

With urbanisation still growing strongly, Belgium is no an exception to the need to meet the challenges of tomorrow. Consequently, the desire to make the transition to intelligent cities emanates from the politicians who run our country and our cities. However, with the possible exception of Brussels, Belgium does not have any cities considered as megacities where major innovations are urgently needed and where the means of financing are more substantial. Belgium, on the other hand, has cities of all sizes and where the challenges to be met are unique and adapted to particular situations. So we are talking about Smart Cities but also Smart Territories in order to apply the projects to a larger territory with more people. Belgium remains an innovative territory but is far enough away from the cities that lead the global dynamic in terms of Smart Cities[48]. As a result, the policies in charge of cities have, for several years now, accelerated innovation projects to close this gap, which is still far too wide. In this section, we will briefly report on Belgian cities projects in order to visualise where we are in terms of Smart Cities.

For example, the Smart City Institute, in a survey on Belgian cities[40], identified a number of innovative projects that have already been put in place. First of all, the SmartNodes concept has been implemented in the city of Wavre in the Walloon Region. This project is part of the "Smart Environment" category and aims to reduce the electricity consumption of urban lighting. This intelligent lighting has been implemented in a pilot housing estate with many houses and, unlike conventional lighting, SmartNodes only switch on when pedestrians, bicycles or vehicles cross the street. The street lamps are interconnected and can therefore adapt their lighting to the situation at time "t". The intensity of the lighting is also adapted to the target to be illuminated, thus limiting unnecessary lighting. This solution therefore drastically reduces energy losses[97] and, therefore, reduces the impact on the environment. This innovation is also positive for the economy and mobility because it reduces consumption costs and allows the infrastructures to be adapted to the mobility of the city.

Another innovative solution, found here by the municipalities of Brussels, is the "Fix My Street" application[87]. This application, which is freely accessible to citizens, consists of counting the places to be improved in the Brussels municipalities[40]. This platform is based on the engagement of citizens who can use the platform to denounce urban degradation such as tags on walls, holes in roads or lack of lighting due to broken light bulbs. All these remarks are geolocalized and competent services for each problem are called in order to mitigate as soon as possible these permanent damages in our cities. This application therefore helps to govern better while involving citizens in this sense. The data of these incidents are therefore listed on a map and allow politicians to resolve these incidents as soon as the necessary funds are available[83].

1.3.2 Smart Cities in the world

Smart Cities are also strongly present in the world. Indeed, there is even a ranking of these cities called the "Smart Cities Ranking"[56] where they are classified according to their technological advances and their projects carried out in the 6 dimensions that make up the framework of the smart city. Numerous projects have been created in all four corners of the world and have enabled megacities such as New York, Sao Paulo and New Delhi to integrate new technologies into their daily lives. Major Scandinavian cities such as Oslo, Helsinki and Stockholm are very high in the ranking and have developed car-sharing solutions to reduce traffic congestion and e-health applications to improve the lives of their citizens.

The city of Singapore in Asia is considered as a pioneer of Smart Cities and was the first to market autonomous taxis to drive its citizens through the city. The Singapore authorities decided to create these taxis to meet the ever-increasing demand for mobility at all hours of the day and night. After extensive testing and the use of artificial intelligence software, these intelligent taxis are now able to take their customers to their destination in complete safety[73].

Regarding the "Smart Living" concept, the megacity of Dubai has set up electronic payment services "mPay" and "DubaiNow" to make life easier for its citizens. Indeed, thanks to these innovations, citizens can pay for cultural outings, transport tickets, fines and so on, all with the help of a single application. These innovations make it possible to reduce time-consuming administrative documents and to centralize everything, making life more pleasant and liveable[65].

The projects are very numerous and varied, and it is unthinkable to draw an exhaustive list. The purpose of this chapter was to explain the concept of Smart City and to give the main components of it. These brief examples from Belgium and elsewhere were therefore mainly intended to make this concept concrete for the reader. Other examples will be reported later in this work and will be related to the theme of this work; facial recognition.

Chapter 2

Data, a gold mine ?

After providing a framework with the first chapter on the definition and main objectives of a Smart City, this second chapter aims to focus on the use of data within the Smart City.

First, it will list the different technologies used to collect data and visualize how these data are collected in the Smart City. These data will then be analyzed in order to improve city life.

Next, we will focus on the privatization of data and how we can protect ourselves against some cyberattacks. The issue of privacy is more than ever at the heart of the debate and it is, therefore, paramount to legislate the technologies inherent to Smart Cities.

Finally, it will be question of pointing out some problems concerning data collection and providing solutions for improvement so that the technologies can be implemented in such a way as to guarantee respect for privacy and data security for all citizens.

2.1 Data Collection

Smart Cities are full of new technologies to improve daily life and these technologies are therefore collecting millions of data continuously. Data are therefore the basic building block of Smart Cities and is collected in order to be scrupulously analyzed afterwards.

According to[57], data are "what is known or accepted as such, on which reasoning can be based, which serves as a starting point for research". The data are therefore the starting point for obtaining information and drawing conclusions from it. There are several formats and types of data making the concept quite complex. First of all, there are the so-called "primary" data, where the data has been collected for a specific research purpose, and in contrast, there are the so-called "secondary" data, being data first collected for another research purpose and then reused afterwards[54]. The technologies used in Smart Cities collect both primary and secondary data.

Then we have quantitative data that can be measured using a scale and categorized, and qualitative data that are not quantifiable. Finally, we come to differentiate between structured and unstructured data. Unstructured data are raw data, i.e. data collected in a format that is not directly usable for analysis. This type of data is mostly present and generated by our human actions. As far as structured data is concerned, which is the rarest, the Smart City Institute[57] tells us that "it is data whose characteristics and presentation allow it to be easily processed and consulted".

Data sources are numerous in Smart Cities, making the data collection architecture complex and difficult to reach a consensus. A non-exhaustive list of these data sources include, for example, artificial intelligence mechanisms, the notion of the Internet of Things or IoT, and intelligent sensors. These technologies are interconnected via the ICT infrastructure that makes up the intelligent city and allows mass data collection. These data can also be open, which we will also discuss in this chapter.

After having been collected by various means, the data are stored in most cases via Cloud Computing. This huge sample of data or mega-data is called Big Data. Big Data analysis therefore refers to the methods of data analysis that enable us to find solutions and services that are suitable for the smart city. These numerous interconnections between data collection, storage and analysis make the data infrastructure quite complex, but this infrastructure is the basis for the functioning of Smart Cities, as we can see in Fig 2.1.

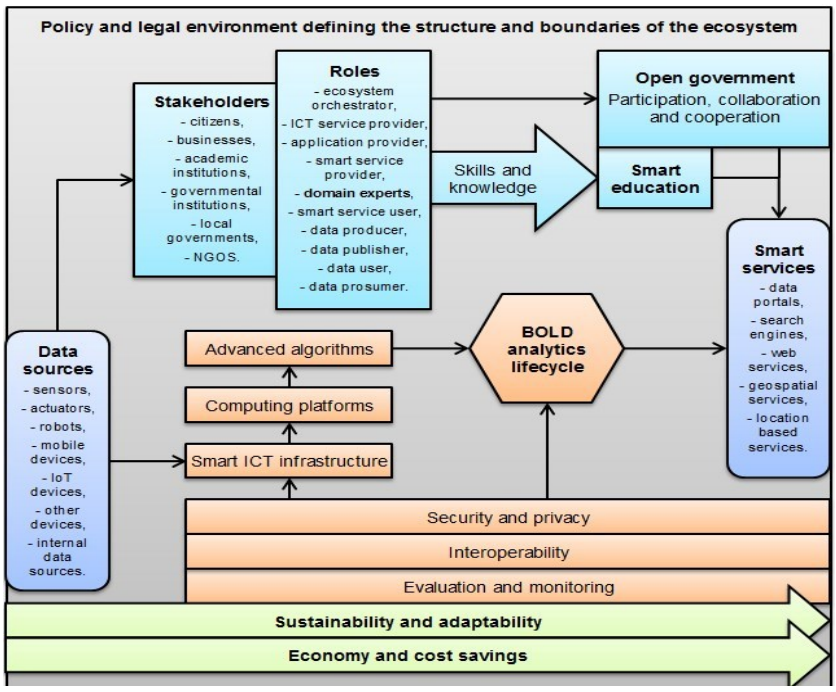


Figure 2.1: Data collection technologies[70]

2.1.1 Internet of Things

Data collection in smart cities is fundamentally based on what we call the Internet of Things or IoT, which is a network of interconnected objects. Thus, according to Mercator[74], the IoT can be defined as "objects that capture, store, process and transmit data, that can receive and give instructions, and that have the capacity to connect to an information network. This network is called the Internet of Things (IoT) and we can distinguish between wearable, mobile, domestic or leisure, infrastructure or productivity objects".

The subject of IoT is very broad, but we can summarize this concept to a set of physical objects that are connected to each other by different technologies and produce and exchange large amounts of data. These interconnected objects are numerous and present in particular in our smartphones, our smart watches but also in what we call sensors, sensors that arrive massively in our cities. Thus, according to the Gartner research institute[47], by next year Smart Cities will have more than 10 billion connected objects, offering authorities and private companies a large growth and an attractive market to follow. As a result, the data generated by these connected devices can either be collected for in-depth analysis but can also be real time data, sent directly to citizens without being stored in giant databases[57].

The Internet of Things is, therefore, the main source of data collection and can be seen as the first layer in the data architecture[2] in the Smart City. The first layer is, therefore, the physical layer, i.e. the physical objects where data are collected (see Fig 2.2.).

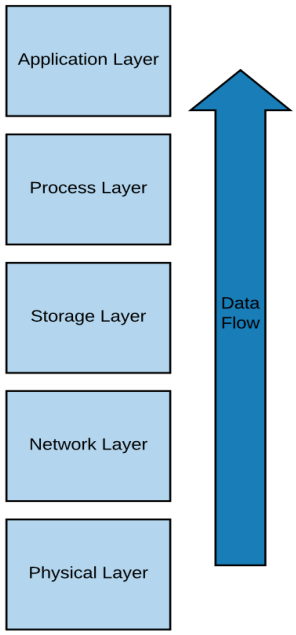


Figure 2.2: Data Layers Architecture

Wearable devices

Connected objects are an integral part of our lives today. This is particularly true of our smartphones, which we use every day, constantly generating millions of usable data. Social networks are, therefore, huge sources of data and are very accurate. Indeed, these data are often geolocalized and specific to each citizen because of his personal use.

These smartphones are interconnected and therefore exchange certain data. However, wearable technologies do not stop at smartphones. Indeed, it can also be a connected piece of jewellery such as a watch for example, or an electronically connected item of clothing. The fields of application of these wearable technologies are limitless, including connected watches in the health sector to monitor vital patient data in real-time for example[84].

Thus, these wearable devices are a first big source of data when we discuss about the Internet of Things. Data harvesting on smartphones using telecommunication networks remains the easiest and cheapest way of implementation because they run on existing devices. We can think of course of social networks but also of mobility or transport applications[43].

Sensors

Sensors are nowadays one of the major sources of data collection. These sensors are mostly located on cars and urban infrastructure. For example, buildings composed of many intelligent sensors allow to collect data on different variables such as temperature, humidity or energy use in order to be able to control these uses and make buildings as efficient as possible[33]. In addition, sensors are also present inside our homes, on our household appliances, allowing us to collect data and improve our quality of life.

Intelligent sensors are also interconnected and can exchange data to improve the lives of citizens. For example, sensors on public roads are ways for reducing energy pollution by communicating with each other to control public lighting according to traffic. On the other hand, intelligent sensors communicate to collect data on urban pollution and the parking problem in order to solve these problems after in-depth analyses[3]. Thus, according to Julien Broue[20], sensors "allow us to convert physical parameters into electronic signals to make them understandable by humans as well as by autonomous systems: light, pressure, temperature, humidity, mould, and many other parameters can now be measured by our sensors to give us a better knowledge of our environments and enable us to adapt each decision according to the different signals".

The Internet of Things is, therefore, everywhere in our lives and collects data on our phone calls, the air quality in our cities or the way we drive. The important point with these physical entities is that they are connected to each other allowing a continuous flow of data exchange. Therefore, these interactions of sensors and devices can be seen as a complex and gigantic network[41]. These objects therefore interact with each other via a network, which constitutes the second layer of our data architecture, the communication network layer (Figure 2.2.).

2.1.2 Artificial Intelligence

The concept of artificial intelligence has also gained momentum in recent years. The AI mechanisms inherent in the smart city use algorithms to better manage data collection. The simple collection of data has no real interest and therefore, artificial intelligence allows a better management of the collected data. Therefore, for Futura[61], AI "consists of implementing a number of techniques to enable machines to mimic a form of real intelligence. AI is being implemented in a growing number of application areas". Artificial intelligence thus transforms the data collected so that we can use it to good effect by extracting information that is essential to the development of solutions that improve life in the city.

AI is also based on learning or even self-learning by copying human reasoning and then improving its functionalities thanks to its experiences and failures[57]. Thanks to one of its branches, namely deep learning, AI can even copy human neural networks through machines. Artificial intelligence therefore makes good use of the collected data but collects itself a lot of data in order to continuously improve the services delivered in Smart Cities.

The available technologies using artificial intelligence are very numerous and for some specialists, the limits of discovery are limitless. The fields of application are also very numerous and make it possible to make the intelligent city more liveable and more sustainable[7]. Among these fields we find for example justice where, using collected data and algorithms, AI mechanisms can make decisions and judgments without human presence, this is what we call Legal Tech[85]. Then, car manufacturers such as Tesla for example are developing autonomous cars entirely based on artificial intelligence to help citizens in their daily transportation[1]. Robots formatted with artificial intelligence are being born all over the world in intelligent cities and help improving the lives of citizens through the services they deliver. Finally, although this list is not exhaustive, we can relate facial and voice recognition using AI via smart cameras or connected objects. This concept of facial recognition is gaining in importance nowadays, and will be further defined and discussed in Chapter 3 of this work.

Ultimately, the set of technologies that make up AI thus allows for targeted use of the data collected and for the collection of more data. In our data architecture (Figure 2.2.), AI can be found in the first layer, the physical layer, because it collects data, but is also in the application layer because it provides concrete solutions for the Smart City.

2.1.3 Open Data, Big Data and Cloud Computing

Cloud Computing

So we discovered the technologies to collect a lot of data and to interact with each other. However, the storage capacities of connected objects and AI mechanisms are sometimes limited and it is therefore essential to be able to store and gather all these data. It is in this context that Cloud Computing is making its appearance and can be visualized as our third layer of our architecture, the storage layer (Figure 2.2.). Thus, according to[69], Cloud Computing "refer to the delivery of on-demand resources and services over the Internet. It refers to the storage and access to data via the Internet rather than via the hard disk of a computer. It thus contrasts with the concept of local storage, which consists of storing data or launching programs from the hard disk". Ultimately, the Cloud is both centralized and decentralized storage, using the Internet as a storage medium.

Cloud computing is composed of three categories, namely Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS), and the cloud can be private, public or hybrid[42]. The good integration of the cloud with IoT objects therefore solves the data storage problem and completes the data architecture[41]. In addition, the cloud makes it possible to deliver information to users without encumbering their storage and this technology is, therefore, very efficient and not expensive.

Cloud Computing stores data for Smart Cities so that they can analyze and process it, making processing much simpler. In addition, the cloud can provide project-specific resources tailored to the needs of citizens and stakeholders.

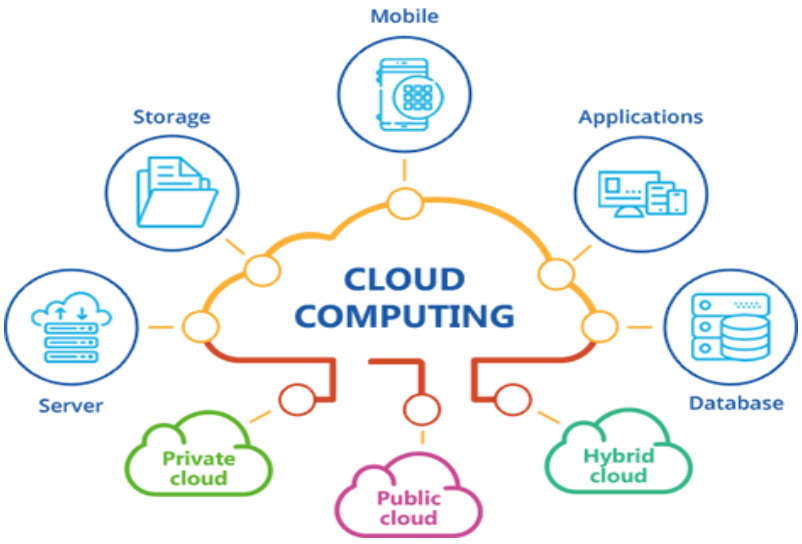


Figure 2.3: Cloud Architecture[9]

Big Data

The data collected and stored are, therefore, very numerous and take up a lot of space. All of these data or "megadata" is known as Big Data. This large set of data, is not the only meaning of the term Big Data, because the Big Data also describes all the advanced techniques for analyzing and processing this massive data in order to complete projects; it is Big Data Analytics. Thus, according to[75], Big Data Analytics is "a set of techniques and technologies that require new forms of integration to uncover large hidden values from large datasets that are diverse, complex and of a massive scale". Mega-data analyses, in order to be considered as such, must fulfill 4 main characteristics[41]:

- Volume : "The amount of all types of data generated from different sources and continue to expand. The benefit of gathering large amounts of data includes the creation of hidden information and patterns through data analysis"[52].

- Variety : "The different types of data collected via sensors, smartphones, or social networks. Such data types include video, image, text, audio, and data logs, in either structured or unstructured format"[52].

- Velocity : "The speed of data transfer. The contents of data constantly change because of the absorption of complementary data collections, introduction of pre- viously archived data or legacy collections, and streamed data arriving from multiple source"[52].

- Value : "Refers to the process of discovering huge hidden values from large datasets with various types and rapid generation"[52].

The collected raw data can be directly analyzed, but algorithms can also perform further sorting and analysis in order to increase the information potential. The Big Data can also be linked via the Cloud to artificial intelligence, thus enabling data analysis solutions and services to be multiplied tenfold[57].

Ultimately, Big Data brings together both considerable data and all the analysis tools that enable decision-makers and public authorities in Smart Cities to facilitate the deployment of intelligent solutions. With regard to our data architecture shown in Figure 2.2, the Big Data is on the penultimate layer, i.e. the process layer, as it relates to the last step before the implementation of intelligent solutions for citizens.

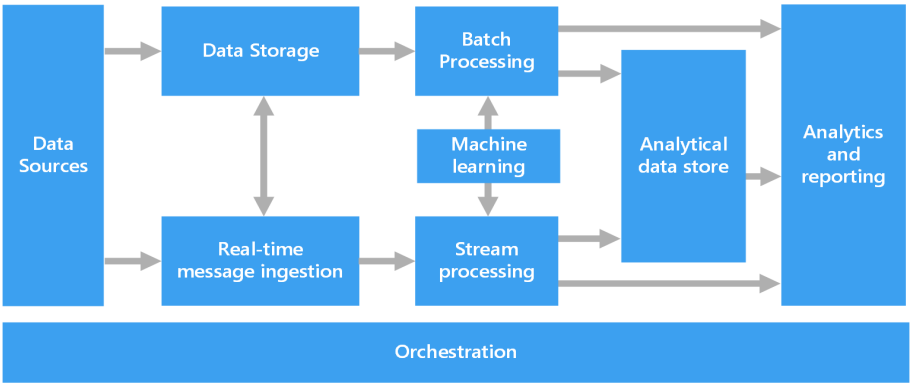


Figure 2.4: Big Data architecture[22]

Open Data

In parallel to this data collection and analysis, which is mostly private, some data are disseminated in open access for the general public. Indeed, the concept of open data is a notion that is deeply rooted in the Smart City dimension and allows citizens to feel included and concerned by the decisions taken. Thus, according to[46], open data is defined as "data that can be freely used, re-used and redistributed by anyone - subject only, at most, to the requirement to attribute and sharealike".

The primary purpose of Open Data is that it is open, i.e. available for free access in order to collect it, use it, or even share it with others. This open data can come from different sources and applied to many fields such as health, environment or culture. However, in order to be qualified as open data, they must, according to the Open Knowledge Foundation, meet 3 criteria[46]:

- Availability and access : "the data must be available as a whole and at no more than a reasonable reproduction cost, preferably by downloading over the internet. The data must also be available in a convenient and modifiable form"[46].
- Reuse and distribution : "the data must be provided under terms that permit reuse and redistribution including the intermixing with other datasets. The data must be machine-readable"[46].
- Universal participation : "everyone must be able to use, reuse and redistribute — there should be no discrimination against fields of endeavour or against persons or groups. For example, 'non-commercial' restrictions that would prevent 'commercial' use, or restrictions of use for certain purposes (e.g. only in education), are not allowed"[46].

These three criteria to qualify Open Data, lead us to the notion of interoperability inherent to this technology. Interoperability is in fact the ability to mix several types and forms of data regardless of their origins and to allow technological tools to work together. Open access data can therefore be mixed easily and allow the retrieval of much more relevant information than without it.

The main advantage of open data is that it offers a high degree of transparency by public authorities with regard to the data collected. This information, which is seen as public, can therefore be considered as common property by citizens who can appropriate it. This new means of governance, called open governance[11], fits perfectly with the vision of the Smart City because it allows the integration of new technologies by including citizens in the decisions. In addition to having visibility over data, citizens can use it and take part in the functioning of the city.

Open data thus contributes to the development of Smart Cities and the strategies of this technology are more and more numerous. All these technologies that we have been able to discover allow us to collect and analyze data in order to bring innovative solutions to our cities. Moreover, these technologies work hand in hand for a better integration and understanding among citizens. So open data remain the spearhead of the Smart City but these open data are not necessarily mega data and these mega data, the Big Data are not necessarily all open.

Data collection and analysis in Smart Cities are quite complex and the technologies communicate a lot with each other. For the sake of clarity, the data flow modeling can be visualized below in Figure 2.5.

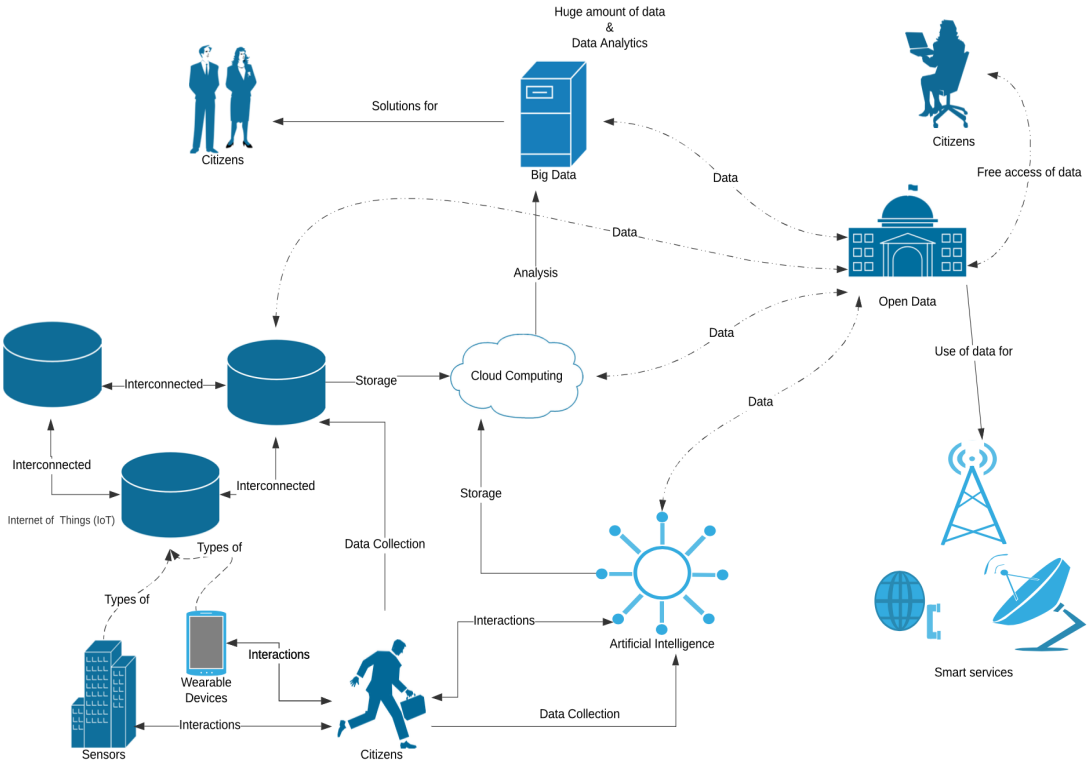


Figure 2.5: Data Flow and Interactions in Smart Cities

2.2 Data Management

We therefore visualized how data are collected in Smart Cities in order to implement innovative solutions to improve the lives of citizens. However, it would clearly be utopian to think that these data can be collected freely without posing a risk to the privacy and security of citizens' data. Indeed, although technological advances bring many benefits, the data and the uses to which they are put are very regularly a threat to the privacy of citizens. Moreover, security breaches can sometimes occur, making citizens and their data vulnerable to cyber-attacks.

Nowadays, with more and more interconnected objects, we are more concerned than ever about the use of our data. Recently, there has been talk of regulating the use of our data by the world's major corporations. Indeed, the GAFAM[38] have recently been obliged to guarantee the respect of the privacy of its users and to be transparent in the use of the data. Data security and privacy are applicable everywhere, as we have noticed during the CoVid-19 pandemic that we are going through this year. The Belgian government has tried to develop a tracking application to fight against the pandemic but this poses a problem because the personal data collected on citizens will be kept for 30 years. All this, is of course an invasion of privacy.

Threats and abuses related to the abusive collection of data are more than ever present in Smart Cities. Stakeholders therefore have an obligation to guarantee the security and privatization of data within their city in order to give citizens confidence. The integration of new technologies cannot therefore take place without preventive thinking to secure data and guarantee a high level of privacy for citizens. The threats are therefore numerous, but solutions also exist. These solutions can be found when the distinction between data security and data privacy is made. Indeed, although these terms are closely related, they do not mean the same thing and do not have the same objective either. Therefore, this section will focus on defining data security and data privacy within the smart city.

2.2.1 Data Security

When we talk about data protection, the terms security and privacy come up very often. These two terms are regularly, erroneously, mixed up and seen as two equal things. However, although these two terms are linked and allow for better data management, they need to be differentiated. Indeed, privacy cannot exist without security beforehand, whereas data can be secured without respecting privacy[43]). Data security is therefore the basis for ensuring the integrity of privacy.

Thus according to[72], Data Security "is focused on protecting personal data from any unauthorized third-party access or malicious attacks and exploitation of data. It is set up to protect personal data using different methods and techniques to ensure data privacy. Data security ensures the integrity of the data, meaning data is accurate, reliable and available

to authorized parties". While data privacy focuses more on the "What", security focuses more on the "How". Data Security therefore aims to solve the technical problem behind the use of the data, referring to the mechanisms to be adopted in order to keep the data confidential. Data security is therefore the first step in data protection, as we can see in Figure 2.6. This security is therefore a set of mechanisms to protect citizens' data from the threat of cyber-attacks. The main objective of companies in this context is to ensure that malicious persons cannot access user data. These data breaches, which are very real threats in the applications implemented in Smart Cities, can be resolved through access controls or encryption for example[44]. These solutions are all based on the CIA model of data security[43]. This CIA mechanism allows to preserve data and prevent data leakage.

- Confidentiality "ensures that data is accessed only by authorized individuals"[21].
- Integrity "ensures that information is reliable as well as accurate"[21].
- Availability "ensures that data is both available and accessible to satisfy business needs"[21].

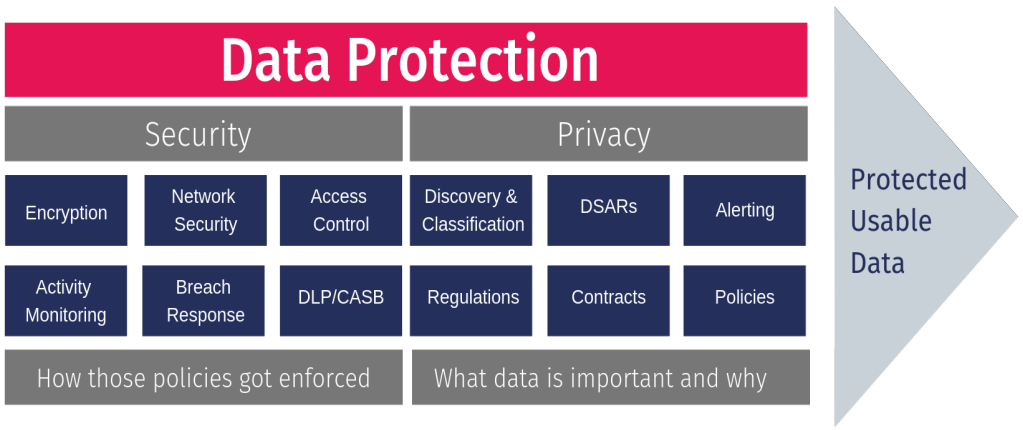


Figure 2.6: Data Protection[72]

Data security cannot be managed by citizens alone, but by companies and public services. These entities must therefore, by any means, make every effort to ensure that citizens' sensitive data remain confidential and secure. Citizens and their data, sometimes collected in open access, are targets for cyber-attacks and this security must be the main objective when creating intelligent applications.

Threats and leakages

As we have seen throughout this chapter, there are many technologies available for data collection. These technologies are interconnected and exchange data, which can increase the number of threats and the risk of cyberattacks[10]. Indeed, every device has a risk of being attacked, but if that device is part of a network, then the whole network becomes vulnerable to that attack and the hacker can infest other devices[4]. A simple vulnerability on a connected device can become an entry point for the cybercriminal to attack the entire network. According to[10], these permanent interconnections "create a system of systems, the complexity of such collaborating systems increases exponentially. As a result, the number of vulnerabilities in a Smart City system will be significantly higher than that of each of its sub-systems".

Open Data and IoT exchange data sometimes openly and are characterized by ease of transmission, but this open data also makes hacking much easier for malicious people. Data Mashup[43] has many advantages, but when data is crossed and some of it are infected, the impact of hacking is even greater on citizens' data. There are many types of cyberattacks that undermine data security in Smart Cities, but the Smart City Institute identifies five major ones[57]. First of all, we have "Malware" which is software designed to infect user data. Second, we have two types of attacks; those based on the web and those based on mobile applications. Finally, we have what we can call "Phishing"[57] and DDOS[27].

The cyberattacks mentioned above can come from anywhere. Indeed, according to[43] [4], the attacks can be internal, i.e. coming from "Service Providers" or "Involved Parties", but these attacks can also come from people external to the manipulation of the data. Their motives may be diverse and varied, but we are seeing an increase in what we call cyberterrorism, i.e. cyberattacks with the aim of a terrorist attack[27]. In addition, threats can come from all types of technology that we can find in Smart Cities. Cybercriminals can, for example, hack into a sensor to transmit false information and data aimed at harming citizens[27]. Hackers can also control smart cameras in order to stop the view on security in the city[27]. Finally, taking the case of open data[27], terrorists could very well collect real-time data on citizens in order to know when it will be the best time for an attack.

Data security is paramount in Smart Cities because, if security is not present, hackers can also harm the privacy of citizens. For example, we can imagine a hacker hacking into a citizen's mobile data and using it without the citizen's consent. There would firstly be a security problem, because the hacker is not a party authorized to use the data, and secondly a privacy problem via the citizen's non-consent to the use of his personal data[43]. In order to guarantee data security, the authorities and companies responsible for technological innovations must therefore aim absolutely to respect the principles of confidentiality, integrity and availability[21]. Fortunately, many solutions exist.

Possible solutions

What concern the solutions to keep our data safe in Smart Cities, many of them exist. We can for example mention the notion of cryptography[43], which takes up many notions and aims to prevent malicious intrusion. Strong passwords or firewalls on ICT applications reduce the risk of data leakage and data breach[4]. Moreover, keeping only reliable networks and reducing the data transmission path are also ways to achieve greater data security[4]. Numerous models for data security have emerged in scientific research, demonstrating the importance that Smart Cities stakeholders should attach to this issue[89].

However, we can point two solutions that are particularly common in many works. First, we have end-to-end encryption[4] which is a type of cryptography. The purpose of this encryption is to ensure a data path between the transmitter and the receiver without potentially harmful intermediaries. These encryptions are mostly based on public keys and can also be "Identity-based" or "Attribute-based"[43] making the security possibilities adapted to each type of technology.

Secondly, many experts agree that it is important to ensure security before problems occur rather than trying to fix them when they have already occurred[4]. The aim should therefore be to test the security of the technological innovations implemented in the Smart City before implementing them for real; this is what we call "Security by Design"[4][43]. As the saying goes, "an ounce of prevention is worth a pound of cure", and therefore this upstream monitoring will allow us to discover the potential threats and leaks that the systems could suffer in terms of security.

Ultimately, the authorities must guarantee the security of the data circulating in Smart Cities in order to give confidence to citizens. Various threats are present and the ubiquity of new technologies and data exchanges make this issue even more complicated. However, the guarantee of security is essential in order to ensure the second part of data protection, namely data privacy. Many solutions exist and good governance in terms of security must definitely take place in order to manage this problem as well as possible.

2.2.2 Data Privacy

Preserving the privacy of citizens is paramount nowadays. According to Figure 2.6, data privacy is the second step in protecting our data and therefore aims to determine which data should be protected and for what reasons. This privacy goes hand in hand with a high-level of upstream security[21]. Data privacy is, therefore, a legislative issue and aims to establish regulations to ensure that the data collected and used respect the privacy of citizens. It therefore aims to determine the way of governance with which data are collected and shared[43]. Thus, according to[72], "Data privacy or Information privacy is concerned with proper handling, processing, storage and usage of personal information. It is all about the rights of individuals with respect to their personal information".

Privacy is a fundamental right and Smart Cities technologies must respect it. Thus, according to the Harvard Law Review[88], privacy is defined as simply "the right to be let alone". This definition has evolved and many authors have sought to define and classify the components that make up the term privacy, making this taxonomy quite complex and extensive[91].

For the sake of clarity, this taxonomy will be based on the 5 types of privacy selected by David Eckhoff[43], relying on different authors[91] [45]. These 5 types of privacy are therefore retained as relevant in order to find solutions to preserve them within Smart Cities :

Type	Explanation
Privacy of Location	"Location information does not only include the location itself but also when and for how long it was visited. Location privacy is usually defined as the protection of spatio-temporal information. Violating location privacy can reveal a person's home and workplace, but also allow inferences about other types of privacy, for example habits, purchase patterns, or health. In addition, co-location information allows inferences about a person's social life" [43].
Privacy of State of Body & Mind	"The state of body and mind encompasses a person's bodily characteristics including biometrics, their health, genome, mental states, emotions, opinions, and thoughts. Violating the privacy of the state of body and mind can lead to discrimination by employers and insurance companies or even to prosecution by totalitarian regimes" [43].
Privacy of Social Life	"A person's social life includes the contents of social interactions, for example what was said in a conversation or posted on a social media platform, as well as metadata about interactions, for example who a person interacts with, when, and for how long. Violating social privacy allows inferences about other types of privacy, e.g., interactions with specialized hospitals or political groupings can reveal information about a person's health or opinion" [43].
Privacy of Behavior & Action	"The privacy of behavior and action includes a person's habits, hobbies, actions, and purchase patterns. When shopping online or when using credit cards, potentially intimate details are shared with retailers. Exploiting this information for other purposes such as targeted advertisement can constitute a violation of privacy. Often, this information allows to draw far-reaching conclusions about the user's life and therefore other types of privacy" [43].
Privacy of Media	"Media privacy includes privacy of images, video, audio, and other data about a person [13]. This includes CCTV and other (knowingly or unknowingly taken) camera footage or media uploaded to the Internet. Redistributing or creating user-related media without consent constitutes a privacy violation" [43].

Table 2.1: Types of Privacy for Data

Privacy Issues

Security breaches or simply bad governance can lead to violations of citizens' privacy. Indeed, even if security is guaranteed between the data exchanged by citizens and the developers of new technologies, citizens' privacy can still be violated[43]. Thus, as exemplified by[66], an autonomous car using a citizen's GPS coordinates can very well be protected via an encryption mechanism, but all data concerning the journey can be collected by the manufacturer against the will of the user. This is of course an invasion of the citizen's privacy and these issues examples are numerous in such cities.

There is a lot of discussion nowadays about citizens' consent to the use of their personal data. However, the Smart Cities, its open access data and its many technologies make privacy very difficult. Indeed, the data coming from connected objects, smartphones or sensors are so numerous that ensuring privacy on all data collected is a major issue in Smart Cities. Some companies looking for profitability through the implementation of intelligent solutions, do not hesitate to use the data of its users, thus endangering part of their privacy[19]. Moreover, according to[19], there is a disparity in the place given to privacy between the public and private sectors making the problems even more numerous.

The data mashup[43] also complicates the respect of privacy because independent data that respect privacy, when they are mixed, could no longer protect citizens and thus open up the possibility of leaks of personal information. Thus, the possibilities of violation of citizens' privacy are numerous and since the preservation of this privacy is important, it is essential to put in place specific policies and regulations in order to solve this problem[43] [4].

Preserving the Privacy of the Citizens

There are many solutions to protect privacy. We can distinguish between technical solutions on the one hand, which are part of a continuous process throughout the data life cycle. On the other hand, we have the legal framework that encompasses this, with the introduction of privacy laws[43].

Privacy by Design & Process

In parallel to "Security by Design", we also have "Privacy by Design" to reduce the threat to privacy through the respect of users' privacy as soon as innovative solutions are put in place[4]. This concept includes seven rules that have to be followed in order to guarantee the respect of privacy from the design stage. These principles are taken up by Cavoukian[26] in her work and are followed by the developers of intelligent solutions:

- Proactive not reactive; preventative not remedial
- Privacy as the default setting
- Privacy embedded into design
- Full functionality with full privacy protection
- Privacy protection through the entire lifecycle of the data
- Visibility and transparency
- Respect for user privacy

This Privacy by Design is therefore a good way to start, but, this concept should be seen more as the first step in a process leading to privacy as the final goal[4]. These rules previously listed by[26], must therefore be incorporated throughout the process, which can be a method of privacy requirements engineering such as PriS[64]. This method, with its own clear semantics, makes it possible to cite the privacy requirements.

The whole process, therefore, aims to be transparent about the use of data, to test and verify whether the technologies are indeed privacy friendly and to make cities and their leaders accountable for the privacy of their citizens[43]. Furthermore, this process can be incorporated into a comprehensive privacy architecture, such as SensorSafe[29].

Other methods applicable to the different technologies can be used to solve the problem of privacy. This non-exhaustive list includes, for example, "Data Minimization", which aims to collect only data relevant to the scope of application. Indeed, whether its the sensors, AI systems or even open data, these technologies often collect more information than necessary, which can lead to over-consumption of data and a risk to privacy[43]. Finally, as a simple applicable mechanism, we can also cite data anonymization such as "k-Anonymity" [94] which allows the collection of a large amount of data while ensuring a high-level of privacy[43] [4]. Other privacy protection mechanisms exist and some are even specific to a particular type of technology. We will come back to this in more depth in Chapter 3, when we will discuss facial recognition.

Legal provisions

Numerous legal provisions have come to surround the preservation of data privacy in Smart Cities. Technological solutions have a lot of advantages, but the law has a much stronger power and is, therefore, an ally in the fight for data privacy. Regions, states, countries and governments have therefore set up strict laws and policies to be respected in order to preserve the privacy of their citizens.

The best known piece of legislation is undoubtedly the General Data Protection Regulation or GDPR[44] which was adopted in 2016 by the European Union[43][57]. This text therefore protects the citizen from data abuse and aims to preserve his privacy as much as possible. The authorities providing Smart Cities solutions are, therefore, required to respect this law and to manage the data collected with care[4].

Other legal frameworks such as the Consumer Bill of Rights[13], the California Consumer Privacy Act (CCPA) in the United States[79] or the HIPAA[43][78] specific to the field of health, allow us to properly regulate the use of our data.

Other less official bodies also advocate for greater transparency, such as those behind the Open Data Charter for example[43]. Privatization of our data is a fight supported by all and strict rules must be applied in order to manage this issue as well as possible and limit abuses[66]. In addition to this desire to guarantee our privacy, many people advocate transparency of algorithms to visualize how our data are used to create intelligent solutions[43].

Chapter 3

AI application : Facial Recognition

After having introduced a study framework with the concept of Smart Cities, its components and its issues, it was a question of relating the different technologies inherent to this concept and the use of personal data that is made of it. Thus, the second chapter dealt with the way in which data was collected and the issues that must be respected in terms of privacy and security.

This third chapter aims to explain a concrete technology integrated in Smart Cities in order to allow the citizens of our future empirical survey to visualize in a concrete way the stakes of personal data protection within our Smart Cities.

It is in this context that we will discuss the concept of facial recognition, which can nowadays enjoy growing popularity. This technology based on artificial intelligence is increasingly present in our cities, and must therefore be clearly regulated so as not to hinder the privacy and data security of citizens.

This chapter therefore aims to exemplify the massive arrival of technology in our cities. First of all, it will be a question of clarifying the global concept of facial recognition. Then, a non-exhaustive list of facial recognition applications will be related and finally, a link with our second chapter will be made in order to understand the issues concerning our personal data, specific to this technology. The framework of Smart Cities, the constraints of personal data protection and a concrete example of technology, will allow citizens to get a concrete idea and an analysis of citizen opinion can then take place.

3.1 The arrival of a new technology

3.1.1 What is facial recognition ?

For many years, we have noted a general desire to make our cities and territories safer. Since then, the introduction of biometrics into our lives has seen the light of day. According to [18], biometrics encompasses all technological applications and methods that make it possible to identify one or more people on the basis of their intrinsic, physical qualities. For example, we can mention fingerprint recognition or iris recognition, which allows a person to be identified with greater or lesser accuracy.

However, this technological recognition requires the willingness of the individual in question to want to be recognized, which limits the scope and proper functioning of these biometric technologies[18]. It is in this context that a particularly powerful new technology has emerged in recent years: facial recognition.

Facial Recognition or Face Recognition can, according to[95], be defined as "a biometric software application capable of uniquely identifying or verifying a person by comparing and analyzing patterns based on the person's facial contours". Facial recognition is based on an artificial intelligence mechanism and therefore a series of algorithms[55], which, after mathematical operations, will allow us to identify a person on the basis of a correspondence[60].

Facial recognition will therefore allow us to identify a person on the basis of a still image or video[102], by performing biometric matches using giant databases. By having a reference image of a person's face, the facial recognition system will compare a new stream of images collected in order to know if the person in these new images is the same person as the one in the reference image[99]. The facial recognition system works like a human brain to compare two things and infer a match or not, this is what we call deep learning[55].

3.1.2 How does facial recognition work ?

There are different systems that create the facial recognition mechanism, but overall we can say that they work with the same central process. In order to allow readers to easily and quickly understand how this technology works, we will not dwell on a non-exhaustive list of the different methods from the scientific literature. We will therefore see with which process matches between images can be made in order to recognize the identity of a person.

First of all, facial recognition can have two main objectives, both using the same operating mode. On the one hand, we have **Verification**. In this case, we will be able to compare a voluntarily chosen individual with the information in the database in order to verify that this person is the right person based on his biometric data[12]. This first mode is also called "one-to-one" because it associates a target person with a precise match. On the other side, we have **Identification**. In this case, facial recognition is going to identify a person who is part of a crowd of other people in order to look for a match in the database and identify who he or she is. This second mode is also called "one-to-many" because it associates an individual with all the individuals in the database and to look for a robust match[12].

Facial recognition can be visualized as a process leading to a positive or negative conclusion of the face comparison. This process involves a series of steps, but first of all, input is needed. This input can either be a still image such as a photograph, or a video filmed by a camera and allowing to have a flow of images in real time[12]. Then, after having obtained a source of images, the facial recognition mechanisms have the following different steps :

- **Face Detection**

Initially, the facial recognition algorithms will aim to detect a face among the source of images obtained[99]. These algorithms will thus allow to differentiate faces from other objects contained in the input. It is clear that the proper functioning of this first step is closely linked and correlated to the quality level of the initial images. Methods inherent to facial recognition algorithms will therefore enable the detection of the characteristics that are predominant in the selection of a face. For the sake of clarity, these different methods will not be explained during this work.

- **Analysis of the face**

In a second step, this previously selected face will be analyzed in order to extract unique characteristics. Each person has an unique set of facial features and this combination will allow for subsequent identification. A widely used method to list the different characteristics is Principal Component Analysis or PCA[102] [98]. This method used on faces in 2D or 3D will allow to complete the matrix of features of the person studied[55]. Thus, geometric characteristics such as the size of the forehead, the distance between the two eyes or the shape of the chin can be identified. The analysis can prove to be extremely precise because, according to[82], the human face has more than 80 nodal points which constitute our facial landmarks.

- **Conversion of the features**

The characteristics collected in the previous step will be converted into data. These data in the form of digit codes will allow the intelligent system to have a unique combination for the face being studied[82]. This numerical code is most often called the faceprint, and this faceprint will be recorded in the database[95]. The transformation of features to specific combination of numbers by deep learning technology can be visualized below[93].

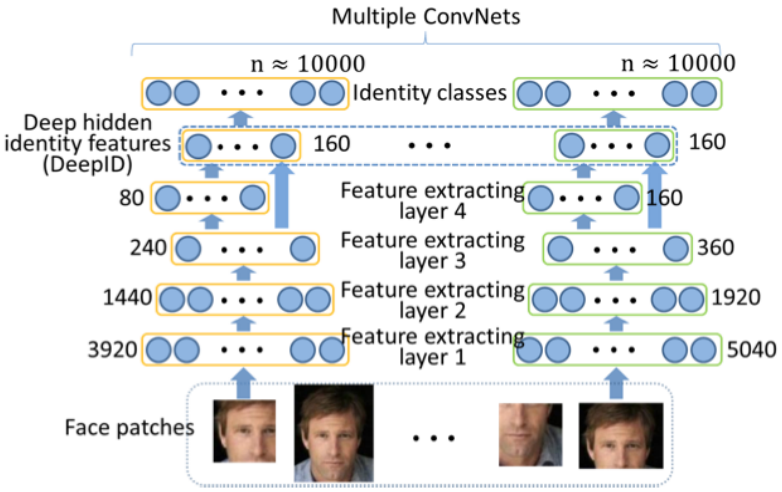


Figure 3.1: Conversion of features into numbers using deep learning[93]

- **Comparison and results**

In a final step, the facial recognition system will compare the single faceprint collected in the previous step with all the faceprints already existing in its database in order to find a match[12]. The algorithm inherent to this technology will then try to find the best match with the highest accuracy according to the features. Thus, finally, a decision can be made whether or not there is a match between the face of the initial photo and a known face in the database[55], which will allow verification or identification. All this process can be visualized as a BPMN process, available on Appendix B.

3.1.3 Limitations of Facial Recognition

Although this technology has many advantages and areas of application, which will be discussed in the next section, there are limitations. Accuracy difficulties can hinder the proper functioning of facial recognition. We can cite a few of them in order to understand the complexity of facial recognition in depth, but this list of limitations is obviously not exhaustive.

First of all, according to[55], the main problem is the variation in the images captured by the cameras. Indeed, the face of the person under study may be subject to movement and therefore different angles of facial posture, which very often complicates the correspondence with a still image in the database. The variation in facial posture and the multitude of facial expressions that a person may have, makes comparison very difficult and thus reduces the probability of finding a match[102]. The face rotation angle and possible facial distortions of the real-time images can be so different from the reference image that the detection threshold of the algorithm is not reached and prevents a true match.

Secondly, the intensity of illumination of the image source has a fundamental impact on the proper functioning of facial recognition[60]. Indeed, lighting that is much too bright or too dark can considerably modify the physical appearance of a face and thus distort the match. Thus, the accuracy of the facial recognition system may be affected if the images collected are taken outdoors or indoors or under extreme lighting conditions.

Other factors may affect proper operation. Indeed, haircut, beard style or the use of glasses can considerably change the overall appearance of a face[98]. The absence or presence of these components in various scenarios will lead to a failure of the facial recognition tool. Lastly, a database with little biometric information will lead to a lack of efficiency because no match can be found[60]. It is therefore necessary to take all these problems into consideration in order to increase the performance of the tool and achieve high accuracy. If this information is not well calibrated and therefore the recognition threshold is not correctly established, this would lead to efficiency problems. For example, we can imagine that a person identical to the person registered in the database but wearing glasses and a large beard might not be recognized by facial recognition technology. In this case, we would have a false negative answer because the tool would give the wrong answer[18].

3.2 Applications of this technology in smart cities

Facial recognition aims to make our cities and citizens' lives safer through a variety of uses. As this technology is constantly growing, the fields of application are, therefore, very numerous. In this section, we will limit ourselves to recounting the main applications of facial recognition in Smart Cities with the help of examples.

Criminal identification

With security as its main objective, facial recognition will allow, thanks to intelligent cameras, to identify among a crowd of people wanted by the police. Whether for minor offences or, as we have experienced more recently, terrorist attacks, smart cameras equipped with facial recognition will be able to identify a wanted criminal[18]. This technology will be of great help to police officers and will assist them in their daily duties. For example, Interpol reports that, thanks to its facial recognition system, more than 650 dangerous fugitives wanted by all the world's police forces have been apprehended[59]. In addition to being able to identify and arrest wanted persons, certain crimes and violence can now be prevented through the use of facial recognition.

Videosurveillance

Artificially intelligent cameras can also make a significant contribution to the daily lives of law enforcement and governments. Indeed, with a global view of their cities in real-time, the authorities are able to manage their actions on a daily basis. Intelligent cameras placed in our streets can, for example, help law enforcement authorities to find missing persons or children on the basis of their biometric information sheet[18]. These cameras installed throughout our cities also make it possible to detect incivilities and, if necessary, to punish citizens who do not respect the laws. Thus, for several years now, China has decided to introduce a social credit system[28]. This system aims at rewarding or punishing, in the form of points, a citizen according to his good or bad deeds and thus to grant him or not services and advantages[16]. Although this system raises citizens' awareness, it is subject to much criticism because it is very often discriminatory if a citizen's social credit is very low. Indeed, if a citizen loses his credit points, he will not have anymore, for example, access to buy a train ticket or visit a museum. This observation makes it clear that this system may not be efficient and, as many people point out, violates the right to privacy and other fundamental rights of citizens.

Access and authorization

Facial recognition can also be used to allow access to public places only to persons authorized to enter them, such as airports[18]. Thus, based on facial recognition at the entrance to boarding gates, the authorities will be able to grant boarding only to persons who have reserved their tickets. This security will make it possible to prevent possible identity thefts and to get the right people in the right seats[92]. This technology will also be able to secure other enclosed public places such as schools or offices. Indeed, smart cameras will be able to collect images of the public place in real time and will detect if unauthorized persons are present in the building in order to emit an alarm[18].

Facial recognition will also be able to secure online access. Indeed, we use our smartphones and social networks intensively everyday. It is in this context that this technology can be used to guarantee access to our personal information only to our own person. The unlocking of our smartphone or the entry in our accounts of social networks using facial recognition, thus makes it possible to guarantee access to the right person at the right time and in complete security[101]. Facial recognition is much more secure than passwords for malicious attacks.

Payments

Payment systems are also subject to facial recognition. Indeed, in some cities, it is now possible to take your metro ticket or cinema ticket via facial biometric detection. This system makes payment easier and faster, which is what many citizens are looking for[68]. Online payments via smartphone are also following suit and many banks are already offering this unique service. Mobile or real payments using facial recognition can considerably reduce the risk of money and bank data theft because they offer a high degree of security[23].

Advertising

Another possible application of facial recognition is the ability to scrutinize citizens' habits in order to develop targeted advertisements. Thanks to smart cameras placed in shopping areas or via facial recognition by smartphone when we use it, companies are able to list what our habits are[18]. Specific advertising spots will therefore be able to appear on our phone screens or on billboards in town to show us the things we like. This is what we call facial recognition marketing[35].

3.3 Towards an invasion of privacy ?

Facial recognition has, as we have seen, many advantages in various fields of application. This technology makes the lives of citizens in Smart Cities considerably safer thanks to its ubiquitous presence in their daily lives. However, many voices are being raised nowadays warning of the extent of facial recognition[31]. Indeed, many people find this technology very intrusive and not very respectful of privacy[18].

First of all, the main criticism that is made is that facial recognition mechanisms track citizens everywhere and at all times. As is the case, for example, in China with their social credit system[28], the slightest actions of citizens are scrutinized and analyzed. However, this problem would lead us to a standardization of surveillance and therefore to an invasion of privacy of each individual[86]. This invasion of privacy must be limited and regulations must be put in place, such as the GDPR, in order to use this technology wisely[31].

The collection of personal data, and in particular biometric data, tells us that the risk of invasion of privacy is very present because these data are used to track us and analyze our behavior[31]. These images and personal information can also be under threat of cyber-attacks and thus data leaks. Facial recognition must therefore be properly secured so that the risks in terms of data theft do not outweigh the advantages that this technology can offer[80].

The introduction of this technology in our Smart Cities must therefore be well framed and regulated in order to preserve the privacy and rights of citizens. One question we can ask ourselves is whether there is an ethical way to introduce facial recognition into our lives and how to achieve it. The consent of citizens and the transparency of public and private bodies using this technology must be scrupulously respected in order to limit the drifts and inconveniences of facial recognition[80]. Citizens, tomorrow's actors of our cities, must ask themselves today about the importance they attach to the security of their data and their privacy. Finally, they must ask themselves whether they are prepared to set aside part of their private life if it is to improve their security in everyday life.

Chapter 4

Citizens and data collection in Facial Recognition

After carrying out a theoretical research on the concept of Smart Cities, the use made of the data and one of the many applications, namely facial recognition, this chapter aims to investigate the theoretical concepts previously discussed.

In this chapter, we will explain how to proceed in order to carry out a survey, from the collection of the numerous data to the analysis of the results. Thus, the elaboration of the study question will be the first step. Then, we will explain the methodology that allowed us to carry out our questionnaire and to be able to collect our data. The final goal of this survey is to infer on the results obtained in order to be able to draw conclusions.

The aim of this chapter is therefore to support the theoretical notions of this thesis with practical experience. We will try to collect the citizens' opinion about the introduction of facial recognition, its applications and its challenges in terms of data security and privacy.

4.1 Context and study question

4.1.1 Context

Thanks to our theoretical literature review, we were able to observe the rise of the Smart Cities phenomenon in our lives. Information and communication technologies will indeed become an integral part of the lives of citizens in the very near future. Among these technologies, we were able to explain the concept of facial recognition by including its applications, its advantages as well as its disadvantages.

In parallel to these notions, we have also addressed the crucial issue of the use of data. Data collection is an integral part of Smart Cities and facial recognition applications, and poses crucial issues. Indeed, via these technologies, there are concrete risks concerning our data in terms of privacy and security. Nowadays, citizens have the right to ask themselves questions about the use of their personal data within the framework of the technologies present in the Smart Cities.

4.1.2 Study Question

The various reflections that have emerged from the context have motivated to deepen the connection between the parts of this thesis. It also seemed important to be able to understand the opinion of those most affected by these technologies, namely the citizens. Indeed, citizens are major actors of Smart Cities and they are the ones who will be able to enjoy the facial recognition applications but they are also the ones who will be under the threat of data theft and violation of privacy. These citizens will be able to improve their security in the city through facial recognition mechanisms but may be vulnerable to data theft and privacy violations. Therefore, it seemed relevant to ask as a study question, **"What is the perception of the privacy versus security trade-off of citizens in smart cities: the case of facial recognition"**.

This study question therefore brings together the concepts discussed in this thesis and seeks to know and understand the opinion of citizens on this subject in order to find a trend. It is also necessary to divide this research question into several sub-questions in order to understand precisely the situation in which citizens find themselves regarding the issue addressed.

First of all, it is important to understand where citizens stand in terms of their knowledge concerning our subject. Since the concepts of Smart Cities and facial recognition are fairly new and complex terms, it is good to know where citizens stand in terms of their knowledge of these terms. In addition, it seems important to know how much citizens know about

them in order to be able to perceive whether citizens can consider themselves experts in these fields. It seems plausible that citizens have already heard about these concepts but do not know more about them, in which case awareness would be high but knowledge of the concepts would be limited. Thus, as a first sub-question, we can ask ourselves:

- **Question 1 : What is the awareness and knowledge of citizens regarding the concepts of smart cities, facial recognition and their current fields of application?**

Then, with the knowledge they have, it was important to find out what citizens thought about the introduction of facial recognition. In trying to understand what is at stake, it is important to understand the position of citizens on the scope of facial recognition they wish to apply and the concrete applications that are important to them. Thus, we can elaborate as a question to be answered :

- **Question 2 : What is the opinion of citizens regarding the introduction of facial recognition mechanisms in our cities and its fields of application?**

In another time, we will look at the notions of data security and privacy. After having discussed these data management issues in Chapter 2 of this thesis, it is obvious that citizens must be aware of the use that is made of their personal data. It therefore seemed important to understand the importance citizens attach to the security and privacy of their data and to apply this to the facial recognition framework. The notion of drifts of these two concepts also needs to be analyzed and we can, therefore, ask ourselves the following question:

- **Question 3 : What is the position of citizens regarding the respect of their privacy and the security of their data in the context of facial recognition?**

Finally, after observing and analyzing citizens' views on facial recognition and the use of their data, it seems relevant to know what their overall positions are. Knowing the possible risks to their data, we will look at whether citizens are willing to let facial recognition become part of their lives. If this is the case, we will seek to observe the nuance that these citizens can issue, what obligations and conditions they have to respect if they accept the arrival of facial recognition in their lives, and where they stand between the dilemma of feeling safe thanks to this technology and keeping their data out of harm's way. It will therefore be a question of whether citizens think that facial recognition and privacy can coexist together, so we can ask ourselves the following question:

- **Question 4 : Are citizens willing to integrate facial recognition into their lives at the expense of a possible invasion of privacy: is there a trade-off, in their view, between feeling safe and keeping their privacy invaded?**

4.2 Methodology

In order to understand and find out the citizens' opinion on the study question and the sub-questions previously mentioned, it was decided to carry out a quantitative study. Indeed, in order to generalize the results obtained in our sample to the population, a maximum number of respondents was necessary. Our sample must therefore be large enough to be as representative as possible. To do this, the quantitative study seems to be the best thing to carry out compared to a qualitative study. The data collection will be done in a structured manner and the data collected will be analysed statistically[50].

4.2.1 Target population and sampling frame

Since the study of this thesis aims to perceive the opinion of citizens regarding facial recognition and the use of their data, it is obvious that the target respondents are citizens. Being limited concerning the answers of non-Belgian people, it was decided that the target population should have Belgian nationality to answer this quantitative study. Furthermore, in order to avoid fear and language barriers but also to obtain honest and thoughtful answers, it was added as a constraint that Belgian citizens should be French-speaking and of older than 18 years old. No other constraints are added in order to obtain answers from citizens of all possible age groups and population classes, with the aim of obtaining robust results that are representative of the entire French-speaking Belgian population.

There is therefore no sampling frame for the target population because it would be impossible to draw up a list of target citizens without adding selectivity bias. A list of French-speaking Belgian citizens would be far too large to draw up and selecting only one group among them would not necessarily cover all age groups.

4.2.2 Survey method

To carry out this quantitative study, a particular method was chosen, namely the electronic survey method via the internet[50]. This method seems to be the most relevant as it allows to obtain many answers quickly. In fact, methods such as face-to-face or telephone interviews will have collected much fewer responses and therefore obtain a sample that is not necessarily representative of the target population. The study will be disseminated on social networks such as Facebook for example[50].

The study is based on an inference of a large number of respondents and therefore this method seems to be the most efficient. Moreover, this method is very advantageous. Indeed, the questionnaire is not administered by the interviewer, the respondent is therefore free and also remains anonymous. The interviewer's bias is therefore very limited at this level. In addition, data collection is fast and access to a large amount of data is possible. The main disadvantage is the fact that the response rate may be low and that the respondents behind the screen may not always answer seriously[50].

4.2.3 Sampling method

With regard to the sampling method, the method of convenience sampling was chosen. This method is a non-probabilistic method that works very well with the chosen survey method. Respondents are therefore chosen at the right place and at the right time via social networks in order to answer the questionnaire[50]. This method is practical and inexpensive but can be subject to self-selection bias.

Thanks to social networks, we can also use the snowball method[50]. Indeed, thanks to the possibility for respondents to share the questionnaire with others, it is possible to reach more people. This method is therefore based on a first sample of people chosen to a certain extent, randomly. These people, through their sharing, also indicate other possible respondents to the questionnaire, which makes it possible to reach even more target people.

In order to obtain a sample that is as representative as possible of the population, it is important that this questionnaire is seen and completed by as many people of different ages as possible. With regard to the size of the sample, it would be essential to obtain at least 150 responses to our questionnaire. However, there is good hope of obtaining more in order to have a sample that is as representative as possible of the population.

4.3 Realization of the questionnaire

Citizens' global information

As a first step, it is important in this questionnaire to focus on the characteristics of the survey respondents. Thus, although the answers remain anonymous, the first set of questions focuses on information about the respondent himself. It is important to give respondents confidence from the outset when completing a questionnaire, and simple questions about their personal information help to achieve this. This personal information is of course limited, but will allow conclusions to be drawn about the target population. Thus, simple questions such as the age group in which the respondent is located, his or her sex, profession and whether the person lives in a rural or urban environment allow information to be gathered while respecting the anonymity of the answers. It is also important to add that this questionnaire was conducted in French. Since the target population is French-speaking Belgian citizens and adults, the choice of language was made in French in order to make it easier for respondents to understand and to perceive all the information and nuances involved. The questions related to this part can be found on Appendix C.

First set of questions

The next step of the questionnaire deals with questions related to our topic of study. First of all, it seemed important to introduce respondents to the concepts of Smart Cities and facial recognition so that they could get an idea of the subject and feel comfortable for answering. The concepts explained in this introduction therefore remain global and do not go into detail, they are only presented for information and understanding.

First of all, it was a question of answering our first study question, which aims to perceive the awareness and knowledge of citizens regarding the concepts mentioned above. Thus, two questions with binary answers aimed to find out whether respondents from the target population had simply already heard about the concepts of Smart Cities and facial recognition. These two questions therefore aimed to situate citizens' awareness on this subject. In a second step, questions with so-called Likert [62] interval scales were drafted to ask citizens to what extent they situate their knowledge about these concepts and their fields of application. All of these questions are available in Appendix D.

Second set of questions

In a second step, we will try to answer our second study question on the opinion of citizens in the context of the introduction of facial recognition in our cities. We will therefore seek to ask them if they are generally in favour of this introduction, if they are confident and what their fears are. We also sought to ask them if they see advantages and disadvantages to this technology and, in their opinion, who are the people responsible for overseeing this technology. Finally, using the scopes of application cited in Chapter 3, we sought to see which of these applications citizens are willing to adopt. All of these questions are available in Appendix E.

Third set of questions

The second part of the questionnaire aims to answer our third and fourth research questions. First of all, in order to facilitate understanding, a brief reminder was sent to respondents regarding the issues in terms of security and privacy of personal data. Secondly, we sought to understand in general terms whether citizens were concerned about the security of their data and the respect of their privacy. We then refocused this opinion on facial recognition in order to see where citizens stand regarding the possible threats that exist. Facial recognition technologies are implemented by governments but also by private companies and, therefore, it was important to question citizens to see which part they trust the most when it comes to security and privacy. All of these questions are available in Appendix F.

Fourth set of questions

Finally, the last part of the questionnaire aims to answer our fourth question we asked ourselves, namely the final position of citizens. Are citizens willing to let facial recognition into their lives and to what extent? Do they find it important that their data is secure and that their privacy is respected? If so, we will ask whether they are confident about facial recognition if safeguards are put in place. Finally, we will look at whether citizens prefer more data security or privacy and whether they prefer to feel safe in their cities or keep their privacy unimpaired. Through these questions, we will aim to nuance this dilemma and to find out whether there is a trade-off between these two extremes for French-speaking Belgian citizens. All of these questions are available in Appendix G.

4.4 Analysis of the results

4.4.1 Sample description

We have therefore collected the responses of Belgian French-speaking citizens and adults over an extended period between 12 July and 27 July 2020. We have tried to satisfy the conditions of the typical respondent population as best as possible so that it is as representative as possible. We therefore wanted to obtain numbers in each age group, in each profession, as well as a good distribution between the sexes and places where they live. After collecting the results, we noticed that 238 respondents from our target population had responded to our survey. This significant figure allows us to continue our analysis.

With regard to the age of the respondents, there are at least 14 respondents in each segment of the population. Young people between 18 and 24 years of age are the most numerous with 33.2% of respondents. This high figure is quite normal as it is partly due to our survey method. Citizens aged 55 and over also responded in large numbers, with 28.6% of respondents. Next came the 45-55 age group with 23.5%, then the 35-44 age group with 8.8% and finally the 25-34 age group was the least represented with 5.9%.

There is a significant disparity between the genders of the respondents since 65.1% of them were women and 34.9% were men. This rather inequitable distribution has, in our opinion, no proven significance and is not due to our survey method. Moreover, 67.2% of the respondents live in the country and 32.8% live in the city. Employees and students are the most represented professions with 42.4% and 32.7% of respondents respectively. Next come retirees with 13.4% and the independents with 7.1%. The liberal professions, the unemployed and the workers are the least represented occupations with 2.5%, 2.5% and 1.3% respectively.

4.4.2 Data manipulation

In order to manipulate the collected data and to be able to analyze them, it was decided to use the program "R Studio". This tool allows to easily import a dataframe and to manipulate the data contained in it. We will therefore, by means of statistical analyses, try to answer our four research sub-questions and finally be able to draw relevant conclusions on our research question.

First of all, since we are focusing on the perceptions of citizens in general, we will conduct univariate analyses for each question in our survey. Thus, the numbers and frequencies of citizens' responses for each question will be extracted and analyzed in order to understand citizens' perceptions and to be able to answer our research questions. As this study is therefore based on the perception of citizens in a global way, we are therefore carrying out what we can call a flat sorting.

In a second step, thanks to data manipulation in R Studio, we will carry out bivariate tests. We will try, as far as possible, to establish links between the characteristics of the citizens in our sample and the answers we were able to collect. Thus, the Chi Squared and Fisher tests will be carried out and will allow us to infer whether there are dependencies between the variables. These results will obviously be relativized because our sample, although consistent at our level, is certainly not entirely representative of the population.

4.4.3 Answers to research questions

Question 1 : What is the awareness and knowledge of citizens regarding the concepts of smart cities, facial recognition and their current fields of application?

First of all, we can observe that there is a significant difference between citizens' awareness about Smart Cities and awareness about Facial Recognition. Indeed, as we can see in Figure 4.1, only 63.4% of the citizens in our sample have already heard about the concept of Smart Cities, while 97.1% of them have already heard about the concept of Facial Recognition.

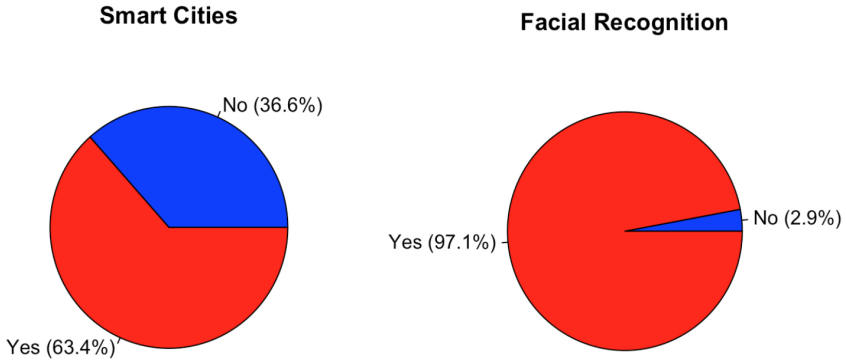


Figure 4.1: Awareness Smart Cities and Facial Recognition

Then, with respect to the results of the other questions available in Appendix D, we obtained the response frequencies available in Figure 4.2. From this table, we can say that a majority of citizens disagree with the assertion that they have a good knowledge of the Smart Cities concept. On the contrary, more than half of the respondents believe that they have a good overall knowledge of the concept of facial recognition. Regarding the knowledge of facial recognition applications, citizens do not think they have a good knowledge of facial recognition applications and therefore mostly disagree with the last two assertions. In addition, we can also note that citizens are very little aware of the technological advances in facial recognition that already exist in Belgium, with barely 17% of cumulative positive responses.

	Strongly disagree	Rather Disagree	Neutral	Pretty much agree	Totally agree	Total
Good knowledge Smart Cities	27.7 % (66)	20.2 % (48)	19.7 % (47)	26.7% (63)	5.9 % (14)	100 % (238)
Good knowledge Facial Recognition	9.3 % (22)	14.7 % (35)	19.7 % (47)	46.6 % (111)	9.7 % (23)	100 % (238)
Knowledge Facial Recognition applications	18.1 % (43)	24.0 % (57)	26.1 % (63)	26.8 % (64)	5.1 % (12)	100 % (238)
Knowledge Facial Recognition applications in Belgium	28.6 % (68)	29.8 % (71)	24.4 % (58)	15.5 % (37)	1.7 % (4)	100 % (238)

Figure 4.2: Frequencies of responses

Then there was talk of cross-firing the data. We therefore seek to verify whether there is a significant dependency between the characteristics of the respondents and their responses. To do this, we conducted Chi Squared and Fisher tests to test the dependencies. We tested the characteristics of the respondents' gender, age group and place of residence. Indeed, we did not have enough respondents in each profession category, so we could not test for addiction with this characteristic. We therefore tested the hypothesis of dependence at a 95% level of reliability (p-value = 0.05).

First, it appears that there is a significant dependency between the gender of the respondent and the knowledge and awareness he or she has about Smart Cities and facial recognition. There is therefore a dependency between the gender of the respondent and the positive and negative answers he or she gave. Indeed, we find that, according to our sample, males have a better awareness and knowledge of concepts. With regard to the age and location of the respondent, there is no dependency with the answers given. We can therefore say that at a level of 95% reliability, there is no link between the level of awareness and knowledge of the respondent with regard to his age and place of residence. In order to answer our first research question, we can draw the following conclusions :

- Citizens have already heard more about Facial Recognition than Smart Cities.
- Citizens have generally already heard of the concepts but are not experts. They do not have as much knowledge as awareness.
- Citizens have an average knowledge of the technological advances involved in facial recognition, but few are aware of the facial recognition technologies that already exist in Belgium.
- The gender of the citizen has an impact on the level of awareness and knowledge. Men have, on average, a better knowledge of facial recognition compared to women.

Question 2 : What is the opinion of citizens regarding the introduction of facial recognition mechanisms in our cities and its fields of application ?

First of all, in Figure 4.3, we can see that half of the citizens are not in favour of introducing facial recognition in Belgium's cities. However, this trend is completely reversed if guarantees in terms of safety and privacy are applied to this introduction of technology. With this constraint, almost 55% of citizens are in favour of the introduction of facial recognition. The citizens in our sample, on the other hand, are not really confident about the introduction of facial recognition. Indeed, more than one citizen in two is not confident and only 5.5% of respondents are very confident. Finally, from this table, we can also note that consent before to the introduction of facial recognition is paramount according to citizens. Indeed, 80% of respondents agree with the assertion that citizens' consent must be introduced.

	Strongly disagree	Rather Disagree	Neutral	Pretty much agree	Totally agree	Total
In favour of the introduction of Facial Recognition in Belgium	20.2 % (48)	28.1 % (67)	25.2 % (60)	21.5 % (51)	5.0 % (12)	100 % (238)
In favour of the introduction of Facial Recognition in Belgium if there are security and privacy guarantees	12.6 % (30)	15.5 % (37)	16.4 % (39)	35.3 % (84)	20.2 % (48)	100 % (238)
Confident about implementation of Facial Recognition	24.4 % (58)	27.3 % (65)	22.6 % (54)	20.2 % (48)	5.5 % (13)	100 % (238)
Citizen consent is paramount prior to implementation of Facial Recognition	5.5 % (13)	5.5 % (13)	10.2 % (24)	20.2 % (48)	58.6 % (139)	100 % (238)

Figure 4.3: Frequencies of responses

With regard to citizens' opinions about the advantages and disadvantages of facial recognition, this opinion is fairly fair, as can be seen on the left side of Figure 4.4. Indeed, almost half of the respondents, 42.9%, think that there are as many advantages as disadvantages regarding facial recognition. Furthermore, 29.8% of respondents think there are more advantages than disadvantages and 24.8% think the opposite, that there are more disadvantages than advantages. Very few citizens hold extreme positions, i.e. only advantages or only disadvantages. On the right side of Figure 4.4, we can see citizens' opinions about the impact that governments and policy makers should have regarding the introduction of facial recognition. The citizens responding to our survey were broadly of the same opinion, 73.9% of them finding that stakeholders should not prohibit facial recognition technologies, but should limit the scope of application. Another 9.7% and 10.5% respectively have a clear opinion that they want to ban these technologies or not ban them at all without any limits on their application.

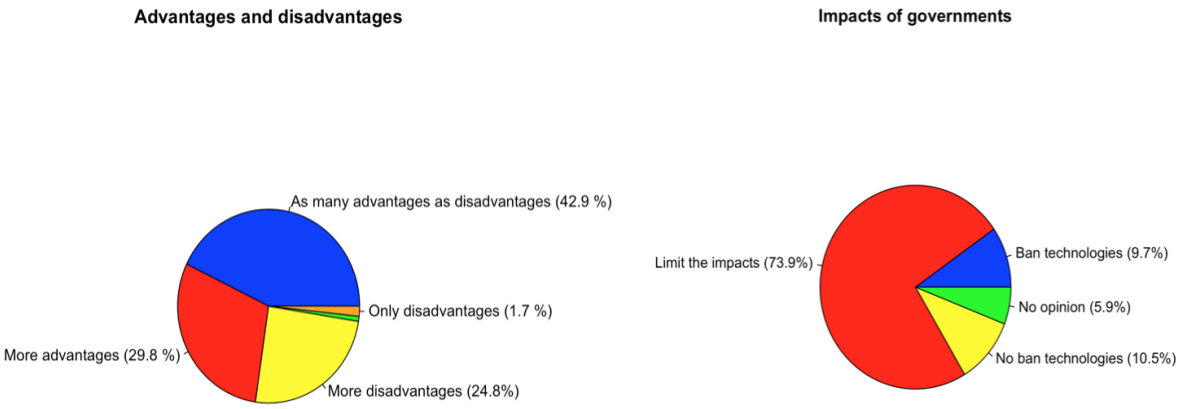


Figure 4.4: Left : Advantages and disadvantages of Facial Recognition.
Right : Impacts of governments and decision-makers

In terms of the applications that citizens are willing to adopt, there is a great contrast between the different applications as we can see in Figure 4.5. Indeed, a large number of citizens are willing to adopt facial recognition as a support for law enforcement to find missing persons (A) and to identify suspicious and dangerous persons (B) with, respectively, 87.8% and 84.5%. Then, more than half of the respondents (56.7%) are in favour of increased surveillance in schools, airports and public places (E). Citizens are 39.9% in favour of introducing facial recognition as a means of safe transaction (F) and 36.1% in favour of continuous video surveillance in cities (G). Then, only 20.6% of respondents are in favour of facial recognition as a means of identification on social networks and unlocking smartphones (D). Finally, very few citizens want facial recognition to be used to create advertisements personalised to their situation (C), with only 3.4% of respondents in favour.

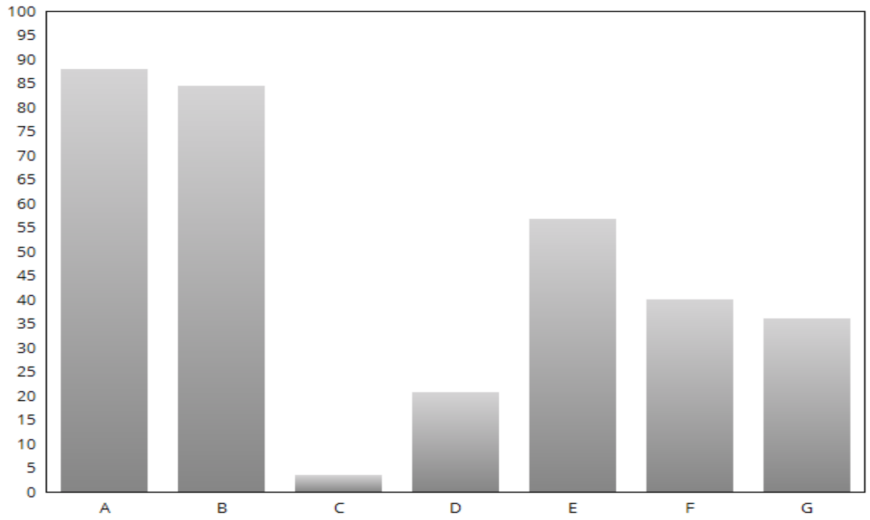


Figure 4.5: Applications of Facial Recognition in Smart Cities

Then we again performed bivariate analyses using Chi-Square and Fisher tests to see if there were any dependencies between the respondents' personal characteristics and the answers they gave. From the analyses we performed, we can say that there is no dependency between the age of the respondent and his or her opinion regarding the introduction of facial recognition. Furthermore, the place where the respondent lives does not have an impact on the opinion he or she holds.

The gender of the respondent has very little impact on the respondent's opinion. Indeed, we found p-values below 0.05 for only two questions. On the one hand, this shows that women have a much less extreme opinion about the introduction of facial recognition if safeguards are introduced. The majority of women are more in agreement with this statement, while the majority of male respondents fully agree with this statement. On the other hand, female respondents are overwhelmingly of the opinion that there are as many advantages as disadvantages in the introduction of facial recognition, while we do not see any trend among male respondents. However, these differences in these two questions do not allow us to say that there is a dependency between the gender of the individual and the opinion he or she has regarding the introduction of facial recognition mechanisms in our cities. In order to answer our second research question, we can draw the following conclusions :

- Citizens are not really confident about the implementation of facial recognition technologies and are only in favour of them if there are guarantees in terms of privacy security.
- Citizens believe that their consent is paramount before implementing facial recognition technologies.
- Citizens do not think there are more advantages or disadvantages regarding facial recognition technologies.
- Citizens believe that governments and decision-makers should limit the impact and scope of applications of facial recognition.
- Citizens strongly favour, as applications, the support of law enforcement to find missing persons and the identification of suspicious or dangerous persons.

Question 3 : What is the position of citizens regarding the respect of their privacy and the security of their data in the context of facial recognition ?

First of all, in order to try to answer this question, we wanted to know whether citizens felt concerned about the use that was being made of their data. Our analysis in Figure 4.6 shows that citizens are generally concerned about their data. Indeed, 35.3% of respondents said they were very concerned about their data and 37.4% were somewhat concerned. A minority of 3.4% do not feel concerned at all and 15.1% feel very little concerned. Finally, 8.8% of respondents feel they should be concerned but admit that they are not concerned at present.

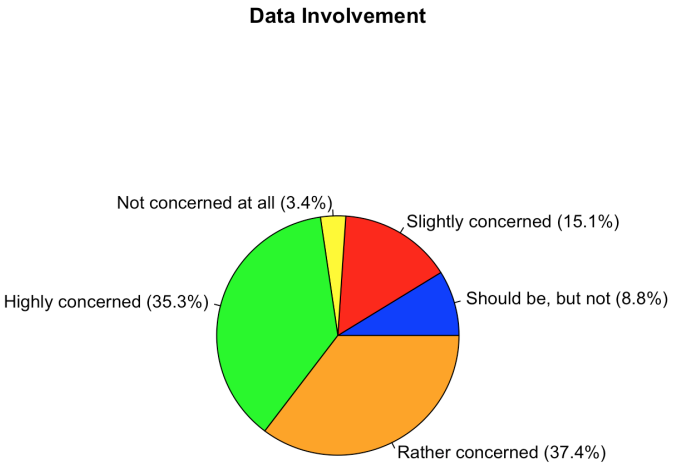


Figure 4.6: Are Citizens concerned by their personal data ?

Secondly, we can see from Figure 4.7. that citizens find it important to respect their privacy through the introduction of laws and regulations such as the GDPR. Indeed, 88.8% of the respondents agree with the statement that the GDPR must be respected in all circumstances to ensure privacy. In addition, more than 7 out of 10 respondents believe that these laws and regulations are essential in the context of facial recognition. From the analysis, it also appears that citizens believe that there are privacy risks in the context of facial recognition. Indeed, 33.2% of respondents fully agree with this sentence and 41.2% agree rather.

As far as data security in the context of facial recognition is concerned, we can say that citizens globally feel concerned. Indeed, 36.6% are very strongly concerned and 37.8% are concerned. Moreover, 76% of citizens believe that there is a risk of data leaks and security breaches in the context of the introduction of facial recognition. Finally, almost 2 out of 3 respondents agree that identity theft is a real threat when we talk about facial recognition.

	Strongly disagree	Rather Disagree	Neutral	Pretty much agree	Totally agree	Total
GDPR must be respected anyway to ensure my privacy	2.5 % (6)	3.4 % (8)	5.5 % (13)	28.6 % (68)	60.0 % (143)	100 % (238)
GDPR and laws governing data are essential in Facial Recognition	4.6 % (11)	5.9 % (14)	16.8 % (40)	29.0 % (69)	43.7 % (104)	100 % (238)
Believe there are privacy risks in Facial Recognition	2.5 % (6)	10.5 % (25)	12.6 % (30)	41.2 % (98)	33.2 % (79)	100 % (238)
Feel concerned about ensuring security of my data in Facial Recognition	2.9 % (7)	7.6 % (18)	15.1 % (36)	37.8 % (90)	36.6 % (87)	100 % (238)
Think there are data leaks and security breaches in Facial Recognition	3.8 % (9)	7.1 % (17)	13.1 % (31)	42.0 % (100)	34.0 % (81)	100 % (238)
Identity theft is a real threat in Facial Recognition	3.8 % (9)	11.3 % (27)	20.2 % (48)	29.4 % (70)	35.3 % (84)	100 % (238)

Figure 4.7: Frequencies of responses

Next, we asked citizens in which stakeholders they trust the most regarding privacy and security in facial recognition (Figure 4.8). Firstly, we found that citizens' opinions are broadly the same regarding both their privacy and their data security. Indeed, a large proportion of citizens, 40% of them, agree that they do not trust governments and the public sector, or companies and the private sector. Secondly, almost three times as many citizens trust governments and the public sector more than companies and the private sector. However, we do see a slight increase in trust in companies when it comes to data security issues.

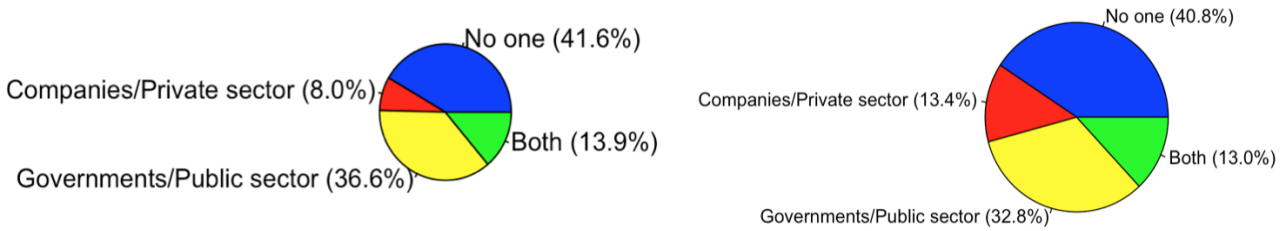


Figure 4.8: Citizens' confidence in stakeholders regarding their data (Left : Privacy , Right : Security)

In a final step, we cross-fired our data on this study question. The first thing we learned from these tests was that the respondent's place of residence does not influence his or her position on privacy and security. However, p-values below the threshold of 0.05 were found for three questions, two related to the gender of the respondent and one related to his or her age.

Firstly, concerning the gender of the respondent, it was noted that this characteristic influences his or her choice in terms of trust in stakeholders concerning the respect of our privacy and the security of our data. Female citizens are more inclined to distrust neither the private nor the public sector, and this choice is favoured by them in the first place. Male citizens, on the other hand, make a choice and trust governments to the public sector as their first choice. Secondly, on the question of whether citizens are concerned about the use that is made of their data, we note a disparity according to age group. Indeed, citizens aged 45 and over are very strongly concerned, while those under 45 are also concerned, but to a much lesser extent. We can therefore assume that the older people are the ones who feel most concerned by their data. However, these dependencies on a few questions do not allow us to say that gender or age influences the position that the citizen has regarding privacy and data security in facial recognition. In order to answer our third question, we can draw the following conclusions :

- Citizens are concerned about the use of their data.
- Citizens believe that laws and regulations governing facial recognition are necessary to ensure their privacy.
- Citizens are concerned about ensuring the security of their data in the context of facial recognition.
- Citizens believe that there are privacy risks as well as data leaks and security breaches in the implementation of facial recognition technologies.
- Citizens generally do not trust the different stakeholders responsible for ensuring their privacy and the security of their data when stakeholders introduce facial recognition technologies.

Question 4 : Are citizens willing to integrate facial recognition into their lives at the expense of a possible invasion of privacy : is there a trade-off, in their view, between feeling safe and keeping their privacy invaded ?

In order to answer this last sub-question of the study, we gathered the citizens' opinion via a few questions available on Figure 4.9. First of all, it emerged that more than 9 out of 10 respondents agree that guarantees in terms of privacy and security must be introduced before facial recognition technologies are implemented. Secondly, almost 50% of the respondents believe that there are too many risks regarding privacy and security for facial recognition to be properly introduced. Subsequently, citizens also agree with almost 60% that governments should regulate facial recognition mechanisms. Finally, when we asked the question whether governments have a responsibility about the use of our data, 46.7% of respondents totally agreed and 37% somewhat agreed with this assertion.

	Strongly disagree	Rather Disagree	Neutral	Pretty much agree	Totally agree	Total
Guarantees of privacy and security must be placed before the implementation of Facial Recognition	0.8 % (2)	2.5 % (6)	6.4 % (15)	25.6 % (61)	64.7 % (154)	100 % (238)
There are too many risks of privacy and security to introduce Facial Recognition	3.4 % (8)	18.5 % (44)	27.7 % (66)	25.6 % (61)	24.8 % (59)	100 % (238)
Governments must regulate Facial Recognition mechanisms	3.8 % (9)	9.7 % (23)	26.0 % (62)	34.5 % (82)	26.0 % (62)	100 % (238)
Governments have a responsibility about the use of my data	1.2 % (3)	4.6 % (11)	10.5 % (25)	37.0 % (88)	46.7 % (111)	100 % (238)

Figure 4.9: Frequencies of responses

The graphs in Figure 4.10. show us the position of citizens on two other issues. On the left, we can observe the level of citizens' favour concerning the introduction of facial recognition if guarantees in terms of privacy and security are put in place. On this graph, we have two poles, point A where the citizen is totally unfavourable to this idea and point E where the citizen is totally favourable, point C being the neutral opinion. We can therefore say, looking at the graph, that the citizens are rather favourable with this idea with more than 50% positive opinions.

On the graph on the right, we looked at whether citizens had a preference between respect for their privacy and the security of their data. Point A being a very strong preference for security, point E a very strong preference for privacy and point C an equivalent preference for both concepts. This shows that citizens attach slightly more importance to their privacy than to their security. However, the majority opinion, with almost 37% of respondents, is an equivalent preference between privacy and security in the context of facial recognition.

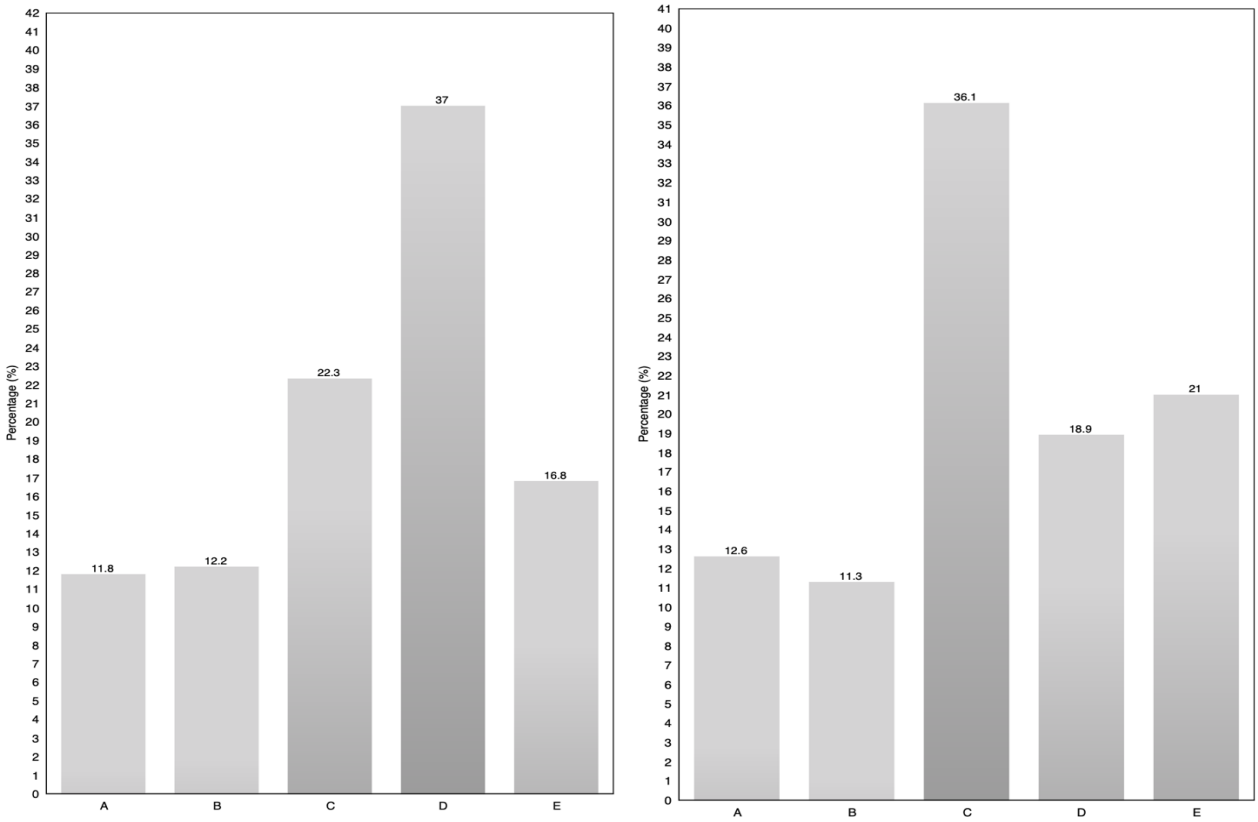


Figure 4.10: Feeling about Facial Recognition (Left). Privacy or Security of Data (Right).

In the last set of questions in Figure 4.11, we can see that citizens do not think that the security of their data is more important than their privacy. The reverse is also true, since they also do not think that their privacy is more important than the security of their data. They therefore put these two issues on an equal footing. Finally, when we asked them whether they are prepared to lose some of their privacy if it is to improve their safety, citizens tend to disagree. In fact, more than half of the respondents are not prepared to lose part of their privacy, 18.9% are neutral and 30% are still prepared to lose part of their privacy if it is to feel safer in the city.

	Strongly disagree	Rather Disagree	Neutral	Pretty much agree	Totally agree	Total
Privacy is more important than Security in Facial Recognition	6.3 % (15)	21.9 % (52)	31.1 % (74)	26.5 % (63)	14.2 % (34)	100 % (238)
Security is more important than Privacy in Facial Recognition	9.7 % (23)	16.8 % (40)	34.9 % (83)	30.7 % (73)	7.9 % (19)	100 % (238)
I'm agree to give up some of my privacy to improve my safety in the city	23.9 % (57)	26.9 % (64)	18.9 % (45)	22.7 % (54)	7.6 % (18)	100 % (238)

Figure 4.11: Frequencies of responses

We then conducted again the Chi-Squared and Fisher tests to test for dependencies between respondent characteristics and their responses to this study question. The results show that there is no dependency according to the age or place of residence of the respondent. The dependency according to the gender of the respondent is very low since only 1 question of the questionnaire is impacted.

Indeed, we found a p-value of less than 0.05 concerning the preference between privacy and security of citizens' data. As a result, the main opinion of female respondents is that there is a clear equivalence between these two concepts, but with a slight advantage for privacy. Male respondents do not have a very clear-cut main opinion, but their tendency is more towards a preference for data security. This difference alone to this question obviously does not allow us to conclude that the gender of the respondent has an impact on the general opinion of our study sub-question. Therefore, in order to answer our last study sub-question, we can draw the following conclusions :

- Citizens are not prepared to feel more secure at the expense of invading their privacy.
- Citizens place as much importance on privacy as on the security of their data.
- Citizens believe that there are many risks regarding privacy and security and that guarantees in this respect should be introduced before implementing facial recognition technologies.
- Citizens believe that governments should regulate facial recognition because they have a responsibility for the personal data collected.
- Citizens are confident in the introduction of facial recognition in our cities only if strict guarantees in terms of privacy and data security are in place.

4.4.4 Answer to our research question

Based on the preliminary findings of our four sub-questions, we can now attempt to answer our research question "What is the perception of the privacy versus security trade-off of citizens in smart cities : the case of facial recognition". The purpose of this research question was therefore to understand the position that citizens take when we talk about Smart Cities, Facial Recognition and the use of their data. It is also worth remembering that the citizens interviewed in this survey were drawn from a sample of the population, and this sample was intended to be as representative as possible.

First of all, we could see that the citizens have already heard about the concepts of Smart Cities and Facial Recognition but are not really aware of the technological advances on this subject, especially in Belgium. However, awareness and knowledge of these concepts are very important because they allow citizens to measure the issues at stake and to express an opinion about the use that can be made of their data.

In a second step, we could see that citizens are not really confident about the implementation of facial recognition and that they plead for strict guarantees in terms of security and privacy. These security and privacy concerns should, in their view, be reduced through citizen consent and government directives limiting the scope of applications. On the other hand, citizens see also in facial recognition some benefits that will make their lives safer, such as assistance to law enforcement and the detection of dangerous persons.

Citizens want to improve their safety in cities but they are also concerned about the use that is made of their data. Citizens believe that there are many risks of privacy breaches and security leakages in facial recognition. They also believe that governments and companies should do everything possible to protect their data before putting facial recognition technologies on the market.

Finally, we can say that citizens want to feel safe, but they are not prepared to let their privacy be violated. As a result, citizens are calling for a trade-off between these two opposites. Indeed, citizens feel ready to let facial recognition into their lives on the only condition that strict safeguards have to be introduced to guarantee the security of their data and respect for their privacy. There are, in their view, many risks concerning this technology and stakeholders must now regulate this technology because they have a responsibility towards our data. It is essential that clear guidelines are introduced to frame this technological breakthrough so as to maximise the benefits while minimising the drawbacks. The precautionary principle is therefore the answer to this research question because, as the saying goes, an ounce of prevention is worth a pound of cure.

Chapter 5

Limits and discussion

5.1 Limits of the study

This study of citizens' perceptions has therefore enabled us to gather a great deal of information and reach certain conclusions. However, it is obvious that our study has limitations. Indeed, we did not have a sampling frame and therefore had to choose our respondents on a somewhat approximate sampling frame. In addition, the sampling method we used was not probabilistic, which would have been ideal in order to obtain the best possible external validity. It is also important to remember that due to certain constraints such as time, money and resources, we used only one survey method, namely the electronic method. This method allows us to collect many responses but there is unfortunately a risk that the respondent, behind his screen, may not always answer honestly. However, we have tried to limit this inconvenience by reassuring the respondent about the complexity of the subject and by limiting the length of the questionnaire.

The main bias that can affect our results is that of self-selection. Indeed, due to the survey method used, i.e. via social networks, it is obvious that younger people are more inclined to be affected. The people most affected by this questionnaire are therefore those who belong to the same age group and, more often than not, the same social class as the interviewer. This is why it is obvious that young people and students are the most represented. This bias can be dangerous as it can threaten the external validity of the study. However, we have tried to reduce it as much as possible. Indeed, through the sharing of this questionnaire, we were able to reach more people from outside the interviewer's environment. Thus, many older people and non-students were able to answer our questionnaire in order to try, to a lesser extent, to obtain a very representative sample. The experimenter's bias was also considerably reduced by the choice of the self-administered questionnaire. Finally, another bias that may impact the internal validity and reliability of the survey is the Halo effect. However, we tried to limit this effect by mixing items in our survey.

5.2 Discussion and future research

In the previous chapter, we were able to analyze the results of our survey and draw conclusions. These conclusions are, at our level, relatively relevant and representative of the population. Thanks to our literary research and the practical application that has been made of it, the reader can now be in a position to grasp precisely all the issues involved in the subject of this thesis. It emerges that citizens will come to question the massive arrival of information and communication technologies and the use that is made of their data.

In terms of the research itself, we can only recommend to go further in analysing citizens' perceptions on this subject. Indeed, it would be judicious to apply this study to a larger part of the population in order to increase the robustness of the results. This target population could also be made more heterogeneous by covering all professions and social classes in order to be more representative of the population's opinion. It would also be a good idea to submit this study to a panel other than that of Belgian French-speakers. In this way, differences of opinion between French-speakers and non French-speakers or between Belgians and foreigners could be found in order to draw relevant conclusions.

In view of the results obtained, we can also ask ourselves how the world of tomorrow will be made, the one integrating these technologies into our lives. Thus, the opinion of the citizens is essential in the framework of Smart Cities and we must aim to respect their demands. However, Smart Cities and the use of data are not limited to Facial Recognition and it would be good to go further in this direction. The opinion of citizens will have to be carefully analysed and listened to in order to integrate these things into our lives in the best possible way. Listening to their demands and understanding their fears would be a good thing and it would be wise to go deeper in this direction.

Finally, a lot of research has already been done on the integration of technologies in our cities and how well they work together. However, given the issues we have addressed in this work, it is clear that this issue goes far beyond our cities. The use of our data now impacts our lives in a significant way and is a current issue in law, politics and industry. It is therefore obvious that a framework for this use must be introduced so that all these systems can live in harmony and respect each other. Data are nowadays a source of richness but also of fears and therefore pushes us to review and rebuild our systemic environment. It would therefore be important to aim to seek a framework that encompasses respect for our data in all these environments and to achieve harmonisation.

Chapter 6

Conclusion

The purpose of this thesis was to link various concepts that have become popular recently. First of all, we could see that the concept of Smart City can be a significant help in meeting the future needs of our cities and territories. Indeed, this concept of the new city allows the efficient integration of information and communication technologies in order to make the life of its citizens better, thanks to its many applications.

Next, we looked at the issue of data collection and management in these smart cities. It is obvious that these technological advances bring many benefits to our lives, but unfortunately there are risks in terms of security and privacy. It is therefore essential that these technologies take place in our lives while ensuring that these concepts are guaranteed.

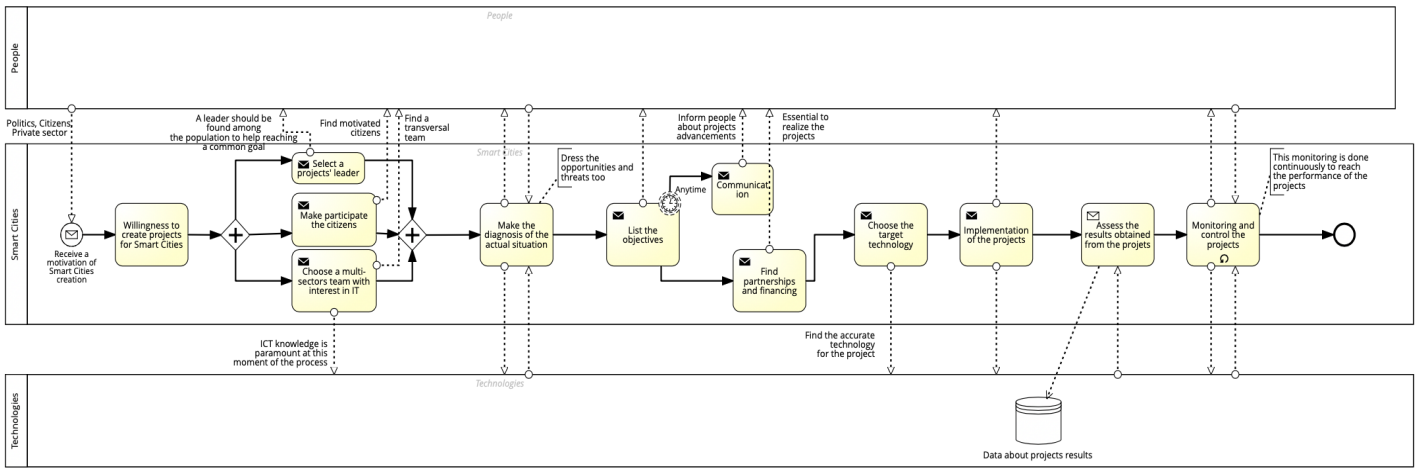
Thirdly, we were able to discover a technological breakthrough that is widespread today, namely facial recognition. We have been able to see that this technology using artificial intelligence has many applications in Smart Cities, making it possible to considerably increase citizens' sense of security.

This theoretical knowledge allowed us to ask ourselves what is the opinion of citizens regarding this information and thus to aim at answering our study question "What is the perception of the privacy versus security trade-off of citizens in smart cities: the case of facial recognition". We have seen that citizens do not have a great deal of knowledge about facial recognition and the applications that are already in use today. It also emerged from this analysis that citizens attach great importance to the respect of their privacy and the security of their data. These citizens are ready to see facial recognition become an integral part of their lives because concrete applications can significantly improve their security. However, in order for this technology, and more generally Smart Cities and technologies, to evolve properly, it is obvious that measures must be taken with regard to our data.

In today's world, with ever-increasing innovation, it seems important to include guarantees before the situation gets out of hand and takes on unwanted proportions and drifts. These technologies are vectors for innovation and continuous improvement in our lives, but it is also important to guarantee our integrity and privacy. Indeed, we are currently going through an unprecedented economic and health crisis. Technological advances will certainly make it possible in the near future to try to return to a stable situation, but it is clear that citizens must be included in these transitions and in this change. It is important for citizens to regain confidence in society and this requires transparency of new technologies in terms of respect for privacy. Therefore, clear regulations governing these technologies seem to be essential and will make it possible to turn these inventions into powerful and indispensable tools for tomorrow's world.

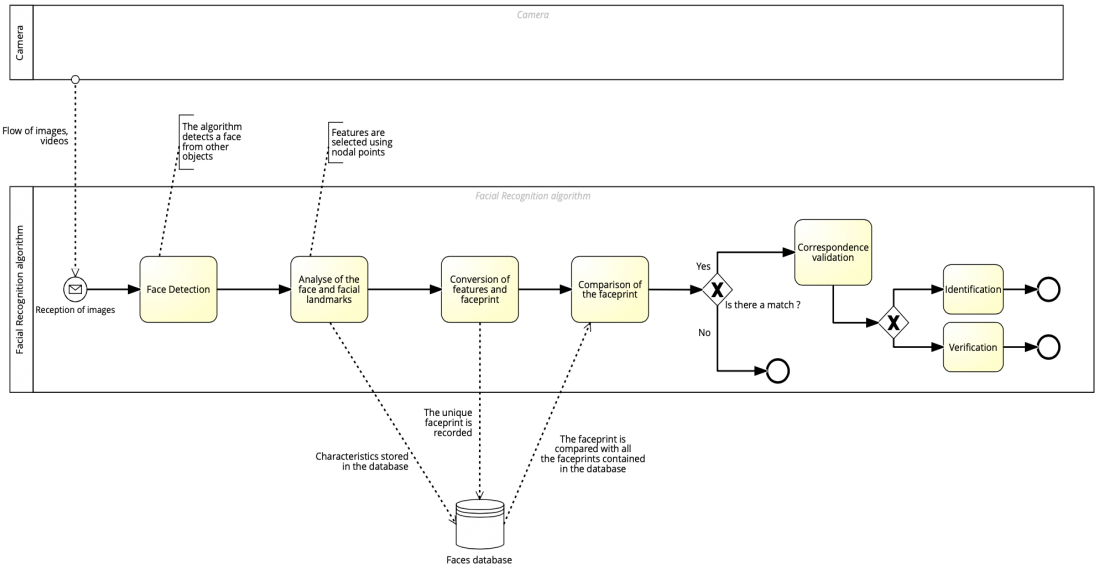
Appendix A

Smart City Process



Appendix B

Facial recognition



Appendix C

Citizens' global information

Formulation of the question	Possible answers	What do we mesure ?
Which age category do you fall into ?	• 18-24 • 25-34 • 35-44 • 45-54 • 55 and above	Age group of the respondent
What's your gender ?	• Male • Female	Gender of the respondent
Where do you live ?	• In the city • In the country	Place of life of the respondent
What is your profession ?	• Student • Employee • Worker • Liberal profession • Independant • Retired • Unemployed	Profession of the respondent

Appendix D

First set of questions

Formulation of the question	Possible answers	What do we mesure ?
Have you ever heard about the concept of the Smart City?	• Yes • No	Raw awareness about Smart City
Have you ever heard about the concept of the Facial Recognition ?	• Yes • No	Raw awareness about Facial Recognition
To what extent do you agree with these statements? A. I think I have a good knowledge of the Smart City concept. B. I think I have a good knowledge of the concept of Facial Recognition. C. I'm aware of the technological advances in facial recognition. D. I have a good knowledge of the facial recognition technologies already existing in Belgium.	Likert's interval scale (5) : 1. Strongly disagree 2. Rather disagree 3. Neutral 4. Pretty much agree 5. Totally agree	Degree of agreement about assertions concerning knowledge of Smart Cities and Facial Recognition

Appendix E

Second set of questions

Formulation of the question	Possible answers	What do we mesure ?
To what extent do you agree with these statements? A. I am in favour of the introduction of this type of technology in our cities in Belgium. B. I am in favour of the introduction of this type of technology in our cities in Belgium if there are guarantees in terms of the security of my data and the respect of my privacy C. I'm confident about the introduction of facial recognition in our cities D. I think the consent of citizens is paramount before this kind of technology is introduced.	Likert's interval scale (5) : 1. Strongly disagree 2. Rather disagree 3. Neutral 4. Pretty much agree 5. Totally agree	Degree of agreement concerning assertions about introduction of Facial Recognition
Please tick the answer that best suits you regarding the possible advantages and disadvantages of facial recognition.	One single answer : • There are only advantages regarding facial recognition • There are only disadvantages regarding facial recognition • There are more advantages than disadvantages regarding facial recognition • There are more disadvantages than advantages regarding facial recognition • There are as many advantages as disadvantages concerning facial recognition	Opinion about impacts of Facial Recognition
Among these different facial recognition applications, please check the ones you would be willing to adopt in our smart cities and territories? (Several answers possible)	Multiple answers : - Support to law enforcement to find missing persons - The identification of suspicious or potentially dangerous persons - The implementation of personalized and targeted advertising based on the citizen's behaviour - Identification on social networks and intelligent unlocking of smartphones - Increased surveillance of schools, airports and public places - The implementation of secure transactions and payments - Continuous video surveillance in all public places	Numbers and types of applications, the respondent is willing to have in the city
What do you think of the impact that our governments and decision-makers should have on facial recognition?	One single answer : • They need to ban facial recognition mechanisms in our cities • They don't need to ban facial recognition mechanisms in our cities • They must limit the fields of application of facial recognition in our cities. • No opinion	Opinion of the respondent about framework of Facial Recognition

Appendix F

Third set of questions

Formulation of the question	Possible answers	What do we mesure ?
In general, to what extent do you feel concerned about the use that may be made of your personal data?	One single answer : • Not concerned at all • Slightly concerned • Rather concerned • Highly concerned • I should be concerned, but I'm not.	Respondent's degree of concern on personal data
To what extent do you agree with these statements? A. I believe that, in accordance with the GDPR, my privacy must be respected regardless of the technology used. B. I find that the RGPD and the laws governing the use of my data are essential to the proper functioning of facial recognition. C. I believe that there are privacy risks in the introduction of facial recognition mechanisms.	Likert's interval scale (5) : 1. Strongly disagree 2. Rather disagree 3. Neutral 4. Pretty much agree 5. Totally agree	Degree of agreement concerning assertions about data privacy in Facial Recognition mechanisms
To what extent do you agree with these statements? A. I am concerned about ensuring the security of my data in the context of facial recognition technology B. I think there is a great deal of risk of data leaks and security breaches in the introduction of facial recognition mechanisms. C. I think identity theft is a real threat in the context of facial recognition data collection.	Likert's interval scale (5) : 1. Strongly disagree 2. Rather disagree 3. Neutral 4. Pretty much agree 5. Totally agree	Degree of agreement concerning assertions about data security in Facial Recognition mechanisms
In the context of the introduction of facial recognition, which stakeholders do you trust the most regarding the respect of your privacy?	One single answer : • To governments and the public sector • To companies and the private sector • To governments, the public sector, private companies and the private sector • None of the above	Position of the respondent concerning the trust accorded to the different stakeholders in term of data privacy
In the context of the introduction of facial recognition, which stakeholders do you trust the most regarding the security of your data?	One single answer : • To governments and the public sector • To companies and the private sector • To governments, the public sector, private companies and the private sector • None of the above	Position of the respondent concerning the trust accorded to the different stakeholders in term of data security

Appendix G

Fourth set of questions

Formulation of the question	Possible answers	What do we mesure ?
To what extent do you agree with these statements ? A. Guarantees in terms of privacy and data security must be in place before facial recognition mechanisms are introduced. B. I think there are too many risks in terms of privacy breaches and security breaches to be able to introduce facial recognition in our cities. C. I think it's up to governments to regulate facial recognition mechanisms. D. I believe that governments and decision-makers have a responsibility for the use of my personal data.	Likert's interval scale (5) : 1. Strongly disagree 2. Rather disagree 3. Neutral 4. Pretty much agree 5. Totally agree	Degree of agreement concerning assertions about Facial Recognition introduction
How do you feel about the introduction of facial recognition if your privacy and data security are guaranteed?	Differential semantic scale (5) : 1. Devaforable 2. ... 3. ... 4. ... 5. Favorable	Position of respondent about Facial Recognition introduction
What would you favour more in the introduction of facial recognition technologies?	Differential semantic scale (5) : 1. The security of my data 2. ... 3. ... 4. ... 5. The respect of my privacy	Position of respondent about Security versus Privacy of data
To what extent do you agree with these statements ? A. I place more importance on respecting my privacy than on ensuring the security of my data with facial recognition technologies. B. I place more importance on the security of my data than on my privacy in the context of facial recognition technologies. C. I'm willing to give up some of my privacy if it will greatly improve my safety in the city.	Likert's interval scale (5) : 1. Strongly disagree 2. Rather disagree 3. Neutral 4. Pretty much agree 5. Totally agree	Degree of agreement concerning assertions about Safety in city versus security and privacy respect

Bibliography

[1] Pradeep Kumar Agarwal, Jitendra Gurjar, Ashutosh Kumar Agarwal, and Ramkrishna Birla. Application of artificial intelligence for development of intelligent transport system in smart cities. *Journal of Traffic and Transportation Engineering*, 1(1):20–30, 2015.

[2] Agoria. Les données, la pierre angulaire des villes et des communes de demain. https://acdn.be/_projects/smartcities/brochures/Whitepaper_Data_FR_Web_nouv.pdf, 2018. Consulted on 2020-05-17.

[3] Bengt Ahlgren, Markus Hidell, and Edith C-H Ngai. Internet of things for smart cities: Interoperability and open data. *IEEE Internet Computing*, 20(6):52–56, 2016.

[4] Rajendra Akerkar. Privacy and security in data-driven urban mobility. In *Utilizing Big Data Paradigms for Business Intelligence*, pages 106–128. IGI Global, 2019.

[5] Suha Alawadhi, Armando Aldama-Nalda, Hafedh Chourabi, J Ramon Gil-Garcia, Sofia Leung, Sehl Mellouli, Taewoo Nam, Theresa A Pardo, Hans J Scholl, and Shawn Walker. Building understanding of smart city initiatives. In *International conference on electronic government*, pages 40–53. Springer, 2012.

[6] Vito Albino, Umberto Berardi, and Rosa Maria Dangelico. Smart cities: Definitions, dimensions, performance, and initiatives. *Journal of urban technology*, 22(1):3–21, 2015.

[7] Zaheer Allam and Zaynah A Dhunny. On big data, artificial intelligence and smart cities. *Cities*, 89:80–91, 2019.

[8] Hege K Andreassen, Maria M Bujnowska-Fedak, Catherine E Chronaki, Roxana C Dumitru, Iveta Pudule, Silvina Santana, Henning Voss, and Rolf Wynn. European citizens' use of e-health services: a study of seven countries. *BMC public health*, 7(1):53, 2007.

[9] Maor Assayag. Distributed system programming cloud computing and map reducce. https://github.com/MaorAssayag/Distributed-System-Programming-Cloud-Computing-and-Map-Reducce, 2019. Consulted on 2020-05-23.

[10] Adrien Bartoli, Juan Hernández-Serrano, Miguel Soriano, Mischa Dohler, Apostolos Kountouris, and Dominique Barthel. Security and privacy in your smart city. In *Proceedings of the Barcelona smart cities congress*, volume 292, pages 1–6, 2011.

[11] Lorena Batagan. Open data for smart cities. *Academy of Economic Studies. Economy Informatics*, 12(1):136, 2012.

[12] Renu Bhatia. Biometrics and face recognition techniques. *International Journal of Advanced Research in Computer Science and Software Engineering*, 3(5), 2013.

[13] Paul Bischoff. What is the consumer privacy bill of rights? https://www.comparitech.com/blog/vpn-privacy/consumer-privacy-bill-of-rights/, 2018.

[14] ROBERTO BOLICI and LUCA MORA. The development process of smart city strategies: the case of barcelona. 2016.

[15] Peter Bosch, Sophie Jongeneel, Vera Rovers, Hans-Martin Neumann, Miimu Airaksinen, and Aapo Huovila. Citykeys indicators for smart city projects and smart cities. *CITYkeys report*, 2017.

[16] Rachel Botsman. Big data meets big brother as china moves to rate its citizens. *Wired UK*, 21:1–11, 2017.

[17] Mauricio Bouskela, Márcia Casseb, Silvia Bassi, and Marcelo Facchina. *The Road toward Smart Cities: Migrating from traditional city management to the smart city.* Inter-American Development Bank Washington DC, 2016.

[18] Kevin W Bowyer. Face recognition technology: security versus privacy. *IEEE Technology and society magazine*, 23(1):9–19, 2004.

[19] Trevor Braun, Benjamin CM Fung, Farkhund Iqbal, and Babar Shah. Security and privacy challenges in smart cities. *Sustainable cities and society*, 39:499–507, 2018.

[20] Julien Broue. 6 technologies indispensables à la smart city. https://www.easypartner.fr/blog/6-technologies-indispensables-a-la-smart-city/, 2018. Consulted on 2020-05-17.

[21] Michael Buckbee. Data security: Definition, explanation and guide. https://www.varonis.com/blog/data-security/, 2020.

[22] Microsoft Build. Architectures de big data. https://docs.microsoft.com/fr-fr/azure/architecture/data-guide/big-data/, 2020. Consulted on 2020-05-25.

[23] Chris Burt. Mastercard working with transport partners on payments via gait or face biometrics. https://www.biometricupdate.com/202002/mastercard-working-with-transport-partners-on-payments-via-gait-or-face-biometrics, 2020.

[24] Silvia Calegari and Elie Sanchez. Object-fuzzy concept network: An enrichment of ontologies in semantic information retrieval. *Journal of the American Society for Information Science and Technology*, 59(13):2171–2185, 2008.

[25] Andrea Caragliu, Chiara Del Bo, and Peter Nijkamp. Smart cities in europe. *Journal of urban technology*, 18(2):65–82, 2011.

[26] Ann Cavoukian et al. Privacy by design: The 7 foundational principles. *Information and privacy commissioner of Ontario, Canada*, 5, 2009.

[27] Cesar Cerrudo. An emerging us (and world) threat: Cities wide open to cyber attacks. *Securing Smart Cities*, 17:137–151, 2015.

[28] Yongxi Chen and Anne SY Cheung. The transparent self under big data profiling: Privacy and chinese legislation on the social credit system. *J. Comp. L.*, 12:356, 2017.

[29] Haksoo Choi, Supriyo Chakraborty, Zainul M Charbiwala, and Mani B Srivastava. Sensorsafe: a framework for privacy-preserving management of personal sensory information. In *Workshop on Secure Data Management*, pages 85–100. Springer, 2011.

[30] Hafedh Chourabi, Taewoo Nam, Shawn Walker, J Ramon Gil-Garcia, Sehl Mellouli, Karine Nahon, Theresa A Pardo, and Hans Jochen Scholl. Understanding smart cities: An integrative framework. In *2012 45th Hawaii international conference on system sciences*, pages 2289–2297. IEEE, 2012.

[31] CNIL. Reconnaissance faciale : Pour un dabat à la hauteur des enjeux. https://www.cnil.fr/sites/default/files/atoms/files/reconnaissance_faciale.pdf, 2019.

[32] Etienne Cointe and Mathias Virilli. La smart city doit être plus qu'une ville intelligente. https://www.maison-et-domotique.com/curation/la-smart-city-doit-etre-plus-quune-ville-intelligente/, 2014. Consulted on 2020-04-12.

[33] Objet Connecté. Bâtiments intelligents : quand l'innovation vient des startups iot. https://www.objetconnecte.com/batiments-intelligents-marche-iot/, 2016. Consulted on 2020-05-17.

[34] Smart City Consortium. Background smart city. https://smartcity.org.hk/en/about-background.php, 2018. Consulted on 2020-04-27.

[35] Emily Cordwell. Facial recognition marketing. https://emilycordwell.com/2019/05/23/facial-recognition-marketing/, 2019.

[36] Renata Paola Dameri. Searching for smart city definition: a comprehensive proposal. *International Journal of computers & technology*, 11(5):2544–2551, 2013.

[37] J Damon, E Denis, and L Strauch. Smart cities. efficace, innovante, participative: comment rendre la ville plus intelligente? *sur¡ http://www. institut-entreprise. fr/les-publications/smart-cities-efficace-innovante-participativecomment-rendre-la-ville-plus*, 2013.

[38] Juan-Carlos Miguel de Bustos. Gafam, media and entertainment groups and big data. *L'internationalisation de la culture, de l'information et de la communication II: l'emprise progressive des industries de la communication sur les industries culturelles et créatives*, page 39, 2017.

[39] Deloitte. Smart cities : Big data. https://www2.deloitte.com/content/dam/Deloitte/za/Documents/risk/ZA_SmartCitiesBig%20Data_%20finale.pdf, 2015. Consulted on 2020-04-27.

[40] Jonathan Desdemoustier and Nathalie Crutzen. Smart cities en belgique: Analyse qualitative de 11 projets. Technical report, Smart City Institute, 2015.

[41] Manuel Díaz, Cristian Martín, and Bartolomé Rubio. State-of-the-art, challenges, and open issues in the integration of internet of things and cloud computing. *Journal of Network and Computer applications*, 67:99–117, 2016.

[42] Manuel Díaz, Cristian Martín, and Bartolomé Rubio. State-of-the-art, challenges, and open issues in the integration of internet of things and cloud computing. *Journal of Network and Computer applications*, 67:99–117, 2016.

[43] David Eckhoff and Isabel Wagner. Privacy in the smart city—applications, technologies, challenges, and solutions. *IEEE Communications Surveys & Tutorials*, 20(1):489–516, 2017.

[44] Lilian Edwards. Privacy, security and data protection in smart cities: A critical eu law perspective. *Eur. Data Prot. L. Rev.*, 2:28, 2016.

[45] Rachel L Finn, David Wright, and Michael Friedewald. Seven types of privacy. In *European data protection: coming of age*, pages 3–32. Springer, 2013.

[46] Open Knowledge Foundation. Open data handbook. https://okfn.org/opendata/, 2016. Consulted on 2020-05-25.

[47] Gartner. Gartner says 5.8 billion enterprise and automotive iot endpoints will be in use in 2020. https://www.gartner.com/en/newsroom/press-releases/2019-08-29-gartner-says-5-8-billion-enterprise-and-automotive-io, 2019. Consulted on 2020-05-14.

[48] Le Soir Geeko. Smart cities : la belgique à la traîne. https://geeko.lesoir.be, 2019. Consulted on 2020-05-06.

[49] Rudolf Giffinger, Christian Fertner, Hans Kramar, Evert Meijers, et al. City-ranking of european medium-sized cities. *Cent. Reg. Sci. Vienna UT*, pages 1–12, 2007.

[50] Wafa Hammedi. Course : Etude de marché - université de namur, 2017.

[51] Colin Harrison, Barbara Eckman, Rick Hamilton, Perry Hartswick, Jayant Kalagnanam, Jurij Paraszczak, and Peter Williams. Foundations for smarter cities. *IBM Journal of research and development*, 54(4):1–16, 2010.

[52] Ibrahim Abaker Targio Hashem, Ibrar Yaqoob, Nor Badrul Anuar, Salimah Mokhtar, Abdullah Gani, and Samee Ullah Khan. The rise of "big data" on cloud computing: Review and open research issues. *Information systems*, 47:98–115, 2015.

[53] Robert G Hollands. Will the real smart city please stand up? intelligent, progressive or entrepreneurial? *City*, 12(3):303–320, 2008.

[54] Joop J Hox and Hennie R Boeije. Data collection, primary versus secondary. 2005.

[55] Gary B Huang, Honglak Lee, and Erik Learned-Miller. Learning hierarchical representations for face verification with convolutional deep belief networks. In *2012 IEEE Conference on Computer Vision and Pattern Recognition*, pages 2518–2525. IEEE, 2012.

[56] IMD. Smart city index. https://www.imd.org/smart-city-observatory/smart-city-index/, 2019. Consulted on 2020-05-09.

[57] Smart City Institute. Nos territoires face aux données et à leur gouvernance. https://orbi.uliege.be/bitstream/2268/239588/1/Smart%20City%20-%20Le%20Guide%20Pratique%20-%20Tome%203.pdf, 2017. Consulted on 2020-05-10.

[58] Smart City Institute. *Smart City : le guide pratique*. http://labos.ulg.ac.be/smart-city/, 2017.

[59] Interpol. Facial recognition - fact sheet. https://www.interpol.int/How-we-work/Forensics/Facial-Recognition, 2020.

[60] Lucas Introna and David Wood. Picturing algorithmic surveillance: The politics of facial recognition systems. *Surveillance & Society*, 2(2/3):177–198, 2004.

[61] JFuturatech. Definition : intelligence artificielle. https://www.futura-sciences.com/tech/definitions/informatique-intelligence-artificielle-555/, 2019. Consulted on 2020-05-17.

[62] Ankur Joshi, Saket Kale, Satish Chandel, and D Kumar Pal. Likert scale: Explored and explained. *Current Journal of Applied Science and Technology*, pages 396–403, 2015.

[63] Sujata Joshi, Saksham Saxena, Tanvi Godbole, et al. Developing smart cities: An integrated framework. *Procedia Computer Science*, 93:902–909, 2016.

[64] Christos Kalloniatis, Evangelia Kavakli, and Efstathios Kontellis. Pris tool: A case tool for privacy-oriented requirements engineering. In *MCIS*, page 71, 2009.

[65] Ashmita Karmakar. E-governance and its role in infrastructure services of uae, case study—dubai. In *E-Governance for Smart Cities*, pages 81–97. Springer, 2015.

[66] Rida Khatoun and Sherali Zeadally. Cybersecurity and privacy solutions in smart cities. *IEEE Communications Magazine*, 55(3):51–59, 2017.

[67] Nicos Komninos. Intelligent cities. In *Electronic Government: Concepts, Methodologies, Tools, and Applications*, pages 4205–4212. IGI Global, 2008.

[68] Dileep Kumar and Yeonseung Ryu. A brief introduction of biometrics and fingerprint payment technology. *International Journal of advanced science and Technology*, 4(3):25–38, 2009.

[69] Bastien L. Cloud computing – définition, avantages et exemples d'utilisation. https://www.lebigdata.fr/definition-cloud-computing, 2017. Consulted on 2020-05-23.

[70] Martin Lnenicka, Renata Machova, Jitka Komarkova, and Miroslav Pasler. Government enterprise architecture for big and open linked data analytics in a smart city ecosystem. In *International Conference on Smart Education and Smart E-Learning*, pages 475–485. Springer, 2017.

[71] Patrizia Lombardi, Silvia Giordano, Hend Farouh, and Wael Yousef. Modelling the smart city performance. *Innovation: The European Journal of Social Science Research*, 25(2):137–149, 2012.

[72] Data Privacy Manager. Data privacy vs. data security [definitions and comparisons]. https://dataprivacymanager.net/security-vs-privacy/, 2020.

[73] Katarzyna Anna Marczuk, Harold Soh Soon Hong, Carlos Miguel Lima Azevedo, Muhammad Adnan, Scott Drew Pendleton, Emilio Frazzoli, et al. Autonomous mobility on demand in simmobility: Case study of the central business district in singapore. In *2015 IEEE 7th International Conference on Cybernetics and Intelligent Systems (CIS) and IEEE Conference on Robotics, Automation and Mechatronics (RAM)*, pages 167–172. IEEE, 2015.

[74] 11ème édition Mercator. Objets connectés - internet of things (iot). https://www.mercator-publicitor.fr/lexique-marketing-definition-objets-connectes, 2014. Consulted on 2020-05-14.

[75] Peter Michalik, Ján Štofa, and Iveta Zolotova. Concept definition for big data architecture in the education system. In *2014 IEEE 12th International Symposium on Applied Machine Intelligence and Informatics (SAMI)*, pages 331–334. IEEE, 2014.

[76] Andres Monzon. Smart cities concept and challenges: Bases for the assessment of smart city projects. In *2015 international conference on smart cities and green ICT systems (SMARTGREENS)*, pages 1–11. IEEE, 2015.

[77] Taewoo Nam and Theresa A Pardo. Conceptualizing smart city with dimensions of technology, people, and institutions. In *Proceedings of the 12th annual international digital government research conference: digital government innovation in challenging times*, pages 282–291, 2011.

[78] Sharyl N Nass. Beyond the hipaa privacy rule: Enhancing privacy, improving health through research. https://www.confidentialitycoalition.org/wp-content/uploads/2011/11/8-Beyond-the-HIPAA-Privacy-Rule-IOM-Study.pdf, 2009.

[79] State of California Department of Justice. California consumer privacy act (ccpa). https://oag.ca.gov/privacy/ccpa, 2019.

[80] Future of Privacy Forum. Privacy principles for facial recogntion technology in commercial applications. https://fpf.org/wp-content/uploads/2019/03/Final-Privacy-Principles-Edits-1.pdf, 2018.

[81] Michael O'grady and Gregory O'hare. How smart is your city? *Science*, 335(6076):1581–1582, 2012.

[82] Nashwan Adnan Othman and Ilhan Aydin. A face recognition method in the internet of things for security applications in smart homes and cities. In *2018 6th International Istanbul Smart Grids and Cities Congress and Fair (ICSG)*, pages 20–24. IEEE, 2018.

[83] Burak Pak, Alvin Chua, and Andrew Vande Moere. Fixmystreet brussels: socio-demographic inequality in crowdsourced civic participation. *Journal of Urban Technology*, 24(2):65–87, 2017.

[84] Lukasz Piwek, David A Ellis, Sally Andrews, and Adam Joinson. The rise of consumer health wearables: promises and barriers. *PLoS medicine*, 13(2):e1001953, 2016.

[85] Sabrina PRADUROUX, Valeria de Paiva, and Luigi di Caro. Legal tech start-ups: State of the art and trends. In *Proceedings of the Workshop on 'MIning and REasoning with Legal texts' collocated at the 29th International Conference on Legal Knowledge and Information Systems*, 2016.

[86] PrivacyInternational. Facial recognition. https://privacyinternational.org/learn/facial-recognition, 2019.

[87] Brussel Region. Fix my street brussels. `https://fixmystreet.brussels`, 2020. Consulted on 2020-05-08.

[88] Jed Rubenfeld. The right of privacy. *Harvard Law Review*, pages 737–807, 1989.

[89] Mourjo Sen, Anuvabh Dutt, Shalabh Agarwal, and Asoke Nath. Issues of privacy and security in the role of software in smart cities. In *2013 International Conference on Communication Systems and Network Technologies*, pages 518–523. IEEE, 2013.

[90] Signavio. Signavio bpmn modelling. `https://www.signavio.com`, 2020.

[91] Daniel J Solove. A taxonomy of privacy. *U. Pa. L. Rev.*, 154:477, 2005.

[92] Luuk J Spreeuwers, Anne J Hendrikse, and KJ Gerritsen. Evaluation of automatic face recognition for automatic border control on actual data recorded of travellers at schiphol airport. In *2012 BIOSIG-Proceedings of the International Conference of Biometrics Special Interest Group (BIOSIG)*, pages 1–6. IEEE, 2012.

[93] Yi Sun, Xiaogang Wang, and Xiaoou Tang. Deep learning face representation from predicting 10,000 classes. In *Proceedings of the IEEE conference on computer vision and pattern recognition*, pages 1891–1898, 2014.

[94] Latanya Sweeney. k-anonymity: A model for protecting privacy. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, 10(05):557–570, 2002.

[95] Techopedia. The complete guide to facial recognition technology. https://www.techopedia.com/definition/32071/facial-recognition, 2020.

[96] Donato Toppeta. The smart city vision: how innovation and ict can build smart,"livable", sustainable cities. *The innovation knowledge foundation*, 5:1–9, 2010.

[97] DSP Valley. Smartnodes' technology in a nutshell. https://www.smartnodes.be/author/team_smartnodes/page/7/, 2015. Consulted on 2020-05-08.

[98] M Alex O Vasilescu and Demetri Terzopoulos. Multilinear image analysis for facial recognition. In *Object recognition supported by user interaction for service robots*, volume 2, pages 511–514. IEEE, 2002.

[99] Li Wang and Dennis Sng. Deep learning algorithms with applications to video analytics for a smart city: A survey. *arXiv preprint arXiv:1512.03131*, 2015.

[100] Xinghuo Yu and Yusheng Xue. Smart grids: A cyber–physical systems perspective. *Proceedings of the IEEE*, 104(5):1058–1070, 2016.

[101] Lihua Zhao and Richard Tsai. Locking and unlocking a mobile device using facial recognition, March 31 2015. US Patent 8,994,499.

[102] Wenyi Zhao, Rama Chellappa, P Jonathon Phillips, and Azriel Rosenfeld. Face recognition: A literature survey. *ACM computing surveys (CSUR)*, 35(4):399–458, 2003.