Smart cities : the tools of a controlled legal revolution

Laurent Archambault , IP/IT Lawyer, member of the Council for civil drones, SELENE Avocats, Paris
Cassandra Rotily, Doctor in public law, University of Haute-Alsace, CERDACC EA 3992

TABLE OF CONTENTS :

Abstract :

The smart city is equipped with a set of sensors that will collect a multitude of data to improve the quality of life of city dwellers. Developing a smart city requires finding the perfect balance between public and private stakeholders on the one hand, and between protection and innovation on the other, with the overriding issue of privacy protection. The emergence of these smart cities is upsetting the existing legal framework. Big data, the purpose of which is the undifferentiated collection of a large amount of information for purposes that are not known in advance, undermines the GDPR and in particular the principle of purpose. Moreover, the legal fragmentation of cyberspace leads to individuals being subject to different risks and degrees of protection. The creation of a "secure e-zone" is therefore necessary to avoid these disparities within cyberspace, which has no physical borders.

A smart city is a city which uses information and communication technologies (ICT) to "improve quality of life, efficiency of urban operations and services, and competitiveness" while taking into consideration "the needs of present and future generations with regard to economic, social and environmental aspects"[1].

This is the concept that the Paris municipal team and its partners have been seduced about, so it seems. Following the announcement by the mayor of Paris, Anne Hidalgo, that so-called autonomous flying taxis would be in service for the 2024 Paris Olympic Games, the ADP group (*Aéroports de Paris*) presented its vertiport model, a platform dedicated to these vertical take-off and landing vehicles (VTOL).

For the CNIL[2], this new way of managing cities includes public infrastructure (buildings, street furniture, home automation, etc.), networks (water, electricity, gas, telecoms), transport (public transport, roads and intelligent cars, carpooling, commonly named soft mobility - cycling, walking, etc.) as well as e-services and e-administration. We can include drones and drone-taxis in the transport sector;

[1] This is the official definition of the "smart and sustainable city", developed in 2015 by the International Telecommunication Union (ITU-T SG 5 FG-SSCi).

[2]National Commission of Information technology and freedom, *Commission nationale de l'informatique et des libertés*

these two categories are necessary to the smart city (delivery of health products, goods, crisis management, etc.), while benefiting from the infrastructures that will be dedicated to them (bases installed on the roofs of buildings or towers or "vertiports", or even on pontoons following the example of the "Urban Air Mobility" plans deployed in certain countries).

After being analysed, it results that the development of smart cities requires finding the right balance between different factors in order to optimise its advantages and limit its disadvantages. This quest for balance will necessarily lead to changes in their legal framework.

I. Balance as the cornerstone of smart city development projects

A balance must be found, between firstly the public and the private actors (A) and secondly between protecting individuals while encouraging technological innovation (B).

A. The need for a balance between public and private actors

Urban services are carried out by public service delegations or public-private partnerships and are subject to the signing of a contract with the concerned public authority. The smart city necessarily changes the relationship between public and private stakeholders. Indeed, some private infrastructures, such as communication infrastructures and in particular mobile telephone networks, will become essential to overall urban functioning[3].

However, companies often try to impose their economic models, some of which are based on the monetisation of individual data and on advertising[4]. As "masters of data", these private players have the capacity to shape the city "according to the interests of a public that is never more than the sum of their customers"[5]. It is therefore necessary for private and public players to have an ethical charter to enable the development of smart cities while respecting the privacy rights of city dwellers[6].

Private stakeholders have been rather reluctant to reveal their operating data. The French Competition Authority has "explicitly recognised the capacity of data to confer market power on economic actors, which may constitute a barrier to entry for new entrants who would not be able to collect all the data necessary to launch a competing service"[7]. However, a company that possesses such an asset and refuses to make it available to others would probably be in a situation of abuse of a dominant position.

The question of the extent of the fair sharing of data between public and private actors then arises. Private actors make certain processed data available in open data because of a legal obligation they have to comply with (on the example of what has been provided for by the Macron law or the nicknamed energy transition law)[8]. In most cases, this open data provision involves the anonymisation of data[9]. However, since data of general interest are anonymised before being made available in open data, the aim is to "open the way for the return of certain fine-grained data to the public stakeholder for

[3] J.-B. Auby, Algorithms and Smart cities: Legal Data, contribution to the colloquium, Public Algorithms, of 12 and 13 Apr. 2018 at the University of Lorraine (Metz), Revue générale du droit online, 2018, n° 29878.

[4] CNIL, The platform of a city. Personal data at the heart of the smart city factory, Cahiers Innovation & Prospective, Oct. 2017, p. 21.

[5] *Ibid*., p. 1.

[6] T. Verbiest, Smart cities and data, Smart tourism file - Guided tour, JT 2019, n° 221, p. 31.

[7] CNIL, The platform of a city. Personal data at the heart of the smart city, p. 32.

[8] *Ibid*, p. 46; Law 2015-990 of 6 August 2015; Law 2015-992 of 17 August 2015.

[9] Therefore, it is a question of allowing the re-use of this anonymised data by all (competitors, public players, researchers, citizens, etc.).

public service missions", on condition that "these data are anonymised when they are made available in open data"[10]. The aim here is to re-establish the "balance of power between certain private actors and local authorities, which would have an effective lever for carrying out public interest missions" by organising the return of quality data to the public actor.

There is also the risk of the administration losing control of the situation, which could be the case "if the construction of an algorithm, which is useful to it, turns out to be carried out by experts who are beyond its control"[11]. The administration's freedom of action is reflected in the questioning of its discretionary power, which is expressed by the use of its discretionary power and the resulting power of derogation. The algorithm must therefore be able to help the decision-maker. However, this situation gives rise to fears that the outcome found by the machine will replace the administration's decision[12]. This problem relating to decisions automatically based on individual profiles is well taken into account in Law No. 78-17 of 6 January 1978 on Data Processing and Individual Liberties, which provides that "no decision producing legal effects with regard to a person or significantly affecting him or her may be taken solely on the basis of automated processing of personal data, including profiling" (with certain exceptions)[13]. Another paradigm arises, that of the coexistence between the protection of the rights and freedoms of individuals while allowing technological innovation.

B. The need for a balance between protection and innovation, also regarding the arrival of 5G in cities

Data, at the heart of the smart city, is essential for its functioning, since it allows the implementation of both "intelligent" infrastructures and services, which meet the needs of citizens. We can even talk about big data[14], as smart cities use algorithms. Thousands of data are thus collected and "aggregated to provide a different result from that of the data taken in isolation"[15].

Urgent questions therefore arise regarding the protection of individuals' rights and freedoms, as some data collected may be qualified as personal data. Should we accept that individuals' data be massively collected in exchange for a free service aimed at transforming urban space? What appropriate safeguards are put in place?

When a city is being transformed, it is necessary to think about privacy by design (General Data Protection Regulation (EU) 2016/679 of 27 Apr. 2016 [GDPR], art. 25), i.e. the protection of individuals' privacy, as soon as connected services are set up. It is therefore necessary for project developers to carry out a privacy impact assessment if the implementation of the service poses a high risk to the rights and freedoms of individuals (RGPD, art. 35). For example, the start-up Placemeter, which initially proposed to count pedestrians passing in the street using the camera of a smartphone placed on a window, has, in this privacy by design approach, developed an algorithm that makes it possible to recognise objects (human forms), and not individuals (recognisable), via deliberately blurred videos[16]. Thus, Placemeter can count passers-by in order to measure an audience for a neighbourhood, without compromising the privacy of its inhabitants.

[10]CNIL, The platform of a city. Personal data at the heart of the smart city, p. 47.
[11]J. Saison and C. Mondou, The augmented administration, JCP Adm. 2018, n° 50, p. 2338.
[12] *Ibid*.
[13] Art. 47.
[14] Big data can be defined as the "collection and aggregation of large masses of data from different sources, with the aim of extracting new information through statistical, descriptive or predictive analysts", D. Bourcier and P. De Filippi, Open Data & Big Data, Nouveaux défis pour la vie privée, Mare & Martin, coll. Droit & Science Politique, 2016, p. 23.
[15] T. Verbiest, Smart cities and data, op. cit.
[16]CNIL, The platform of a city. Personal data at the heart of the smart city, p. 40.

It is also necessary to recall that any local authority or private sector person carrying out a public service mission must appoint a data protection officer (DPO)[17]. Thus, smart cities seem to be "concerned by this novelty, since any initiative - even a private one - of smart cities must be supported by local authorities and must respond to a mission of general interest"[18].

In order to operate its services, the smart city necessarily collects data intensively, with a form of permanence over time. It is important to emphasise that for each service it will be necessary to ensure that the collection of personal data is really necessary. This is the principle of data minimisation laid down in Article 5(1)(c) of the GDPR: data must be "adequate, relevant and restricted to what is necessary for the purposes for which they are processed". Therefore, only data that are strictly necessary for the performance of the task should be collected, according to the purpose principle, and if it is not essential, it is better not to collect it. The data controller is obliged to express in concrete terms the reasons for collecting and processing personal data. Furthermore, such data shall be kept "for no longer than is necessary for the purposes for which they are processed" (GDPR, art. 5, § 1, e). If personal data are no longer needed, it is better to delete them[19].

As far as travel data is concerned, it has the advantage of making the network more fluid. For example, citizens could reduce their travel time. However, there are also many disadvantages, as this geolocation data makes it possible to see where an individual is at a given moment. Thus, one could effectively identify the habits and lifestyle of individuals, hence the interest in being able to count and estimate a flow without collecting personal data.

When possible (particularly for urban traffic management, for example), we should aim for anonymisation of the data collected rather than pseudonymitication, as the latter would allow the individual concerned by the data to be re-identified. The CNIL recommends the creation of structures to assist public authorities in data governance, which would make it possible to certify this anonymisation[20].

The information and consent of individuals (unless there is another legal basis for the processing) are the cornerstone of personal data protection law and remain legal obligations whenever personal data are collected. Due to the large number of systems used, from both private and public stakeholders, as well as data transfers between each of them, consent becomes *de facto* complex to obtain and opaque, especially when data collection is automated. It is therefore necessary to develop techniques to collect this consent more easily. Each citizen should thus be able to oppose the use of his or her smartphone without his or her knowledge for the optimisation of travel flows (inhabitants, vehicles)[21]. However, how can all residents be informed of all the data that may be collected from them in the public space? In the future, it may be wise to think about grouping this information together and not having the individual study the general conditions associated with each service.

The transition from automated to autonomous vehicles requires maximum processing of personal data[22]. It is no longer a question of processing only the data, but the "flow of data specific to the vehicle and the external environment"[23]. In order to raise awareness among professionals in the automotive sector of the need to protect the data of users of connected vehicles, the CNIL has drawn up

[17]G29, Guidelines on Data Protection Officers, 13 Dec. 2016, rev. 5 Apr. 2017, WP 243 rev. 01, p. 6.

[18] T. Verbiest, Smart cities and data, op. cit.

[19] Please note that the regulations sometimes impose a period of data retention. However, for many data processing operations, the retention period is not fixed by a text. It is then up to the person responsible for the file to determine it according to the purpose of the processing.

[20]CNIL, The platform of a city. Personal data at the heart of the smart city, p. 22.

[21] F. Meuris-Guerrero, How to prepare for the emergence of smart cities, CCE 2017, No. 12.

[22]B. Ehrwein and L. Archambault, The autonomous vehicle facing the challenge of personal data protection, L'Argus 2020, No. 7677.

[23] *Ibid.*

a "compliance pack"[24]. This pack provides rules of conduct for manufacturers of increasingly autonomous cars, but also alerts them to their obligations. These include privacy by design: this involves protecting data from the design stage of the vehicle, in particular by setting up easily configurable dashboards, to guarantee that the user has control over his or her data.

The smart city represents a "very large attack surface"[25]; thus, the systems that make it up can become vulnerable to security breaches. The continuity of service in the city must be ensured. 5G should offer maximum network quality at all times for the most sensitive or critical uses thanks to a "network slicing" technique aimed at "maintaining priority slices at a maximum level of quality, even if it means degrading the quality of the others"[26], provided that security flaws in this technology, and the risks of espionage in particular, are limited.

While the tools for balancing the sharing and exploitation of data between public and private players and for reconciling technological innovation with the rights and freedoms of individuals have been understood, the legal framework relating to smart cities is currently suffering from shortcomings and must be called into question.

II. The emergence of the smart city challenges the contemporary legal framework

The legal corpus is necessarily disrupted by the proliferation of technological changes in the city. Faced with this problem, a solution is emerging: the construction of a common global legal framework for cyberspace that defies state borders.

A. The need to adapt the legal corpus to technological change

The installation in the smart city of a multitude of sensors and the presence of these on people, via their smartphone or vehicle, raises a plethora of legal issues.

The question arises of how to adapt public contracts to a city based on innovative processes. Thus, public procurement law and innovation do not mix well. Indeed, the city that wishes to develop an infrastructure or an intelligent system will look for a company to design it. The companies will then need to experiment with solutions to adapt them. The contractual relations will have to be "established in two stages: a first contract for ordering the system and a second contract for implementing the system"[27]. However, this seems complex insofar as the company that designed the system will not necessarily be the one selected at the end of the design phase[28].

Because of the multiplication of stakeholders (telecommunication operators, public social services, etc.), the question of data ownership arises. The Conseil d'Etat considers that "as the law stands, there is no right of ownership of the individual over his or her personal data. [...] the protection of personal data, as conceived by the law of 6 January 1978, Convention No. 108 of the Council of Europe or Directive No. 95/46/EC, is not based on a patrimonial logic but on a logic of rights attached to the person [...]; there is no right of ownership over raw data"[29]. On the other hand, the intellectual

[24] CNIL, Connected vehicles: a compliance pack for responsible data use, 17 Oct. 2017.

[25] CNIL, The platform of a city. Personal data at the heart of the smart city, p. 14.

[26] Usbek et Rica, How 5G can become the engine of the smart city, March 2020, URL: https://usbeketrica.com/fr/article/comment-la-5g-peut-devenir-le-moteur-de-la-smart-city.

[27] A. Philippot and A. Azzi, The smart city: what are the legal and political issues, Tendancedroit.fr, http://www.tendancedroit.fr/la-smart-city-quels-enjeux-juridiques-et-politiques/.

[28] *Ibid.*

[29] Conseil d'État, Annual study 2014, The digital world and fundamental rights, Doc. fr, Sept. 2014, p. 264.

property code recognises a property right for the producer of a database when this constitution "attests to a substantial financial, material or human investment"[30]. This seems paradoxical since economic actors will enjoy a property right on their databases, while the individuals listed in them are not the owners of their data. Thus, it could be envisaged, on the model of literary and artistic property law, that individuals could form collective management companies for their personal data, with a view to negotiating with services that wish to use them, and the profits would be paid back to the partners of these companies[31].

The question also arises of building a genuine "right to digital privacy". Indeed, some authors believe that the right to privacy, introduced by the law of 17 July 1970 to strengthen the guarantee of individual rights of citizens, is no longer appropriate "in the age of smartphones and social networks"[32]. This concept of privacy should be rethought to offer more protection to individuals whose intimacy is now made vulnerable.

Despite the revolution brought about by the RGPD, which has made it possible to make digital actors more accountable, it already appears outdated. Indeed, if we take into consideration the principles of proportionality and purpose, where the collection of data must be proportional to the purpose invoked by the data controller, we can only note that they are already being undermined by the development of big data[33]. These principles are opposed to the characteristics of big data, which are presented as the "5 Vs" (Volume, Speed (*Vitesse* in French), Variety, Veracity, Value)[34]. Indeed, big data "is based on the idea of an undifferentiated collection of a large amount of information, for purposes that are not known in advance"[35]. While data must be kept for no longer than is necessary for the purposes for which they are collected and processed, this principle is the opposite of a connected object whose purpose is, on the contrary, to "collect personal data on a permanent and continuous basis", since the information collected serves to improve the service over time[36]. This legal framework must be questioned in the face of a cyberspace devoid of physical borders.

B. Building a "secure e-zone"

Although there are different models of smart cities around the world, their actors use the same tools. As cyberspace has no physical borders, it is necessary to reflect on a common global legal framework, given the hyperconnection and interconnection of individuals and the international transfer of data.

The problem of the territorial segmentation of provisions relating to the protection of personal data arises. If we take the example of connected objects (in the broadest sense, including automated cars or drones), they will collect data from point A of the globe, then it will be transferred instantaneously to point C to be stored, and then to point B to be analysed. However, "the regulation of personal data protection has a strictly limited territorial scope"[37]. This leads to a "legal fragmentation of cyberspace", which may subject individuals "to different risks and degrees of protection depending

[30] CPI, art. L. 341-1.

[31] Conseil d'État, The Digital world and Fundamental Rights, supra, p. 265.

[32] A. Bensoussan, remarks collected by C. Lisana, The right to digital privacy, Cyberjustice.blog, 28 June 2020, URL: http://cyberjustice.blog/index.php/2020/06/28/le-droit-a-lintimite-numerique/.

[33] M. Lanna, Connected objects and personal data protection: towards a paradigm shift in protection modalities, Rights 2018/2, n° 68, p. 223.

[34] Y. Demchenko, C. De Laat et P. Membrey, Defining architecture components of the Big Data Écosystem, Collaboration Technologies and Systems (CTS), 2014 International Conference on IEEE 2014. 104 à 112.

[35] A. Philippot and A. Azzi, The smart city: what are the legal and political issues? op. cit.

[36] *Ibid*.

[37] *Ibid*.

on their geographical location"[38]. This highlights the need to build a common global legal framework to address these issues.

The adoption of the GDPR is nevertheless a real step forward in this direction, allowing for a broader application of data protection rules. This has "set in motion a movement to renew various state laws"[39] around the world. California passed the California Consumer Privacy Act (CCPA) in 2018, which was undeniably inspired by the GDPR, with the aim of giving Californian residents more control over their personal data[40].

In addition, the GDPR has various legal tools to regulate the transfer of data from European territory to third countries. These include, for example, the adequacy decision (GDPR, art. 45), which is taken on the basis of a global examination of the legislation in force in a State, in a territory or applicable to one or more specific sectors within that State[41]. In the absence of such a decision, transfers may be based on the existence of "appropriate safeguards" (GDPR, Art. 46)[42].

All these initiatives must truly "mark the starting point of a common reflection on the issue of personal data protection"[43].

In conclusion, while the fragmentation of national legislation could hamper the rights of individuals but also be detrimental to technological innovation, the emergence of a "global framework of trust" would finally make it possible to establish a "secure e-zone" on a global scale "enabling individuals to benefit from all the services offered to them, without their rights being compromised"[44]. It remains to find common ground between countries that sometimes have a radically opposed vision in terms of the protection offered to individuals.

Furthermore, the transport sector today represents one of the greatest challenges for the future of smart cities; the increase in the number of vehicles and traffic jams in cities is creating a need for new modes of transport, free from the road and its constraints. To achieve this, the air route is essential:

- Drones will play a key role in supporting numerous applications such as the delivery of health products, goods, police missions, or even firefighting;

- In 2021, an experimental vertiport will be set up at the Pontoise airfield to test drone taxis and all the components of this service: parking areas, energy and maintenance equipment, and even the route taken by future passengers.

[38] *Ibid*.
[39] *Ibid*.
[40] F. Naftalski, S. Revol and A. Costes, The General Data Protection Regulation as an inspiration for the Californian Consumer Privacy Act, Dalloz IP/IT 2021. 168.
[41] CNIL, Data transfers outside the EU: what changes with the General Data Protection Regulation (GDPR), 24 May 2018.
[42] In the absence, "the transfer may finally be carried out by way of derogation from these global framework tools, in particular situations and under specific conditions" (CNIL, Transfers of data outside the EU: what changes with the General Data Protection Regulation (GDPR), supra).
[43]M. Lanna, Connected objects and personal data protection: towards a paradigm shift in protection modalities, op. cit.
[44] *Ibid.*