Privacy and Data-Driven Applications

Joiverdia Arifiyanto[1], Ningrum Natasya Sirait[2], Miratul Khusna Mufida[3], Mohammad Reza[4]

[1,2]*Universitas Sumatera Utara*
[3]*Politeknik Negeri Batam*
[4]*Universitas Gadjah Mada*
Email: joiverdia@usu.ac.id, ningrum@usu.ac.id, vda@polibatam.ac.id, mohammad.reza@mail.ugm.ac.id

ABSTRACT
The emergence of data-driven applications brings new hope to understand and explain many world phenomena. For instance, it helps to explain how the Covid-19 pandemic spread all around the world. The objective of this research is to bridge the potential disclaimer on privacy data usage. In the middle of a crisis, it is important to keep track of how our private data is kept and used to figure out how this pandemic begins and evolves. On one hand, it is important to keep track of every single citizen related to their interaction and mobility. However, once the data is collected, there are two possibilities: it can be an opportunity, or it can be a threat especially related to the privacy of user data and its security and usage. Focusing on describing how the data collection and data usage and security related to the tracking application created, the potential mitigation about the data usage will be analysed, discussed, and elaborated. Inevitably, the technical solution will process personal data (even if pseudonymised), including health data, which is sensitive data. If the evolution were to be different and allow for broader surveillance, the balance of interests would have to be re-evaluated to assess this new purpose. However, the applicable framework seems to be rather largely unknown or misunderstood, and many questions concerning the tracing of the population to contain the pandemic remain unresolved. The lawfulness of such a system will therefore depend on the purpose and legal basis of the processing.

Keywords*: personal data, protection, track, app*

1. INTRODUCTION

Currently, as the Covid-19 epidemic continues to spread, most public health authorities in other countries have developed applications that support contact tracing. [1] The use of this application is to observe the Corona virus infection chain nationally and across borders by completing manual tracing. However, by analyzing what has been done in other countries affected by the coronavirus, these three main mechanisms for exploiting individual personal data have been used at various points of detention. This personal data is collected and processed to find out if someone is complying with detention and eventually a medical search is following the trail of coronavirus contamination.

For example, Indonesia has implemented an app that can retrospectively identify people who may have had close physical contact. When two users of this application, namely PeduliLindungi [2], are within two meters, their cell phones pair via Bluetooth technology. After 30 minutes or more of synchronisation, both devices record the encounter in the encrypted memory cache. In cases where one person is later detected to have a virus or is in contact with a risk group, the Ministry of Health asks users to allow the cache to be decrypted to warn their relatives. In France, the government allows the TousAntiCovid app, which allows it to identify chains of transmission and notify users who may have had potential contact with a person infected with Covid-19 on a voluntary basis. [3] The value of using an app to monitor the spread of the virus is especially important in the phase out of containment to avoid a revival of the pandemic. The idea is to use a Bluetooth tracking system that only collect data when it encounters or is close to the sensor, unlike geolocation devices which will capture data continuously and in a much more intrusive way. With the bluetooth system, data is encrypted on the user's phone, and the user can stay encrypted and deactivated bluetooth connectivity which allows questions about the validity of the retrieved results.

The European Data Protection Board (EDPB) issued an official statement on the processing of personal data in the context of the COVID-19 pandemic on 19 March 2020. [4] The policy statement called the attention to different stakeholders on the fact that while processing personal data in these exceptional times requires the data controllers not to undermine the protection of the personal data of the data subjects and therefore many considerations need to be considered when dealing with personal data in the context of the COVID-19 pandemic.

Hence, many considerations must be considered to ensure the lawfulness of the processing of personal data. Additional rules apply to the processing of electronic communication data, such as mobile location data. National laws transposing Directive (EU) 2002/58/EC of 12 July 2002 (the ePrivacy Directive) provide for the principle whereby location data can only subsequently serve the data controller if anonymised or if consent is given by the data subjects [5]. In the latter case location data can only continue to function under the condition of consent of the data subjects or the adoption of a specific legislative measure demonstrated to be necessary, appropriate, and proportionate in a democratic society. The application of these texts imposes strict requirements in terms of the legality and proportionality of processing operations, those concerning health data or location data. This reminder by the EDPB is not insignificant.[6] Indeed, there is a great temptation to free oneself from the rules on the protection of personal data or even to rule out the application of the Regulation (EU) 2016/679 (General Data Protection Regulation – GDPR), as in the case of the tracing of individuals. However, these rules continue to govern the implementation of such processing, even if limitations are applicable. Data processing during the Covid-19 pandemic must, therefore, comply with the general conditions of lawfulness laid down both by the GDPR and the *Loi Informatique et Libertés No. 2018-493* (France Data Protection Act – FDPA).

2. PROBLEMS

Any technological solution in compliance with personal data protection principles is necessary to guarantee the rights and freedoms of individuals. Yet withal during this period of the Covid-19 pandemic may found the difficulty in applying those principles. The applicable framework seems to be rather largely unknown or misunderstood, and many questions concerning the tracing of the population to contain the pandemic remain unresolved. Therefore, this research refers to the following questions: (i) in which way personal data are collected and processed within the TousAntiCovid application? and (ii) How does the TousAntiCovid application comply with personal data protection principles according to GDPR?

3. RESEARCH METHOD

The priority of this research shall focus on the extensive study of the literature to produce a comprehensive thesis on legal rights and privacy in relation to personal data and protection. It applies a normative legal study [7]. Use of library research data. Secondary data obtained from primary and secondary legal materials inform the study. Primary legal materials consist of laws and regulations related to the protection of personal data. Secondarily, it includes the opinion of the jurist quoted in the literature that supports the framework of thought and analysis of the research object. Second legal source documents are in the form of reading material/books relevant to this research, scientific articles, theses, dissertations, journals, papers and research reports related to the subject of this study. Third party legal materials or supplementary legal materials include relevant reading materials that provide guidance and explanations on the primary and secondary legal materials, such as general dictionaries, legal dictionaries, scientific magazines and journals, as well as relevant materials outside the field of law to support the data needed in the study.

4. DISCUSSION

Tracing, or contact tracing corresponds to the monitoring of certain digital data, used as indicators of the progress or regression of the pandemic for medical purposes. It consists of using telephone data to trace possible Covid-19 contaminations. This technique must be distinguished from tracking, which is more intrusive because it geolocates smartphones. Given the ethical and legal stakes involved, it seems necessary to clarify the debate by presenting the conditions of access to digital data by the judicial authority, the different forms of exploitation of personal data that can be put in place by the administrative authorities as well as the legal framework allowing to reconcile sanitary efficiency and protection of citizens' public liberties. This type of operation, which is based on the principle of tracing, legally consists of access to data contained in an automated data processing system, such as a mobile phone.

Geolocation is a technological means of locating a person, vehicle, or any other object in real-time. [8] This method, which is much more detrimental to civil liberties than mere demarcation at a given time, must be authorised by a written decision that is justified by reference to the factual and legal elements justifying that the operations are necessary. The use of personal telephone data and geolocation in the context of a judicial investigation is closely supervised and subject to permanent control by a judicial magistrate. In the case of the application of tracing, the exploitation of data is based on a public/private partnership with telecommunications operators without a defined legal framework, hence the absolute necessity to ensure that these data are exploited in compliance with the GDPR.

Faced with these problems, two categories of technological tools that can help combat the spread of the coronavirus must be distinguished: the use of aggregated and anonymised data and the use of individualised data. Given the ethical and legal stakes involved, it seems necessary to clarify the debate by presenting the conditions of access to digital data by the judicial authority, the different forms of exploitation of personal data that can be put in place by the administrative authorities as well as the legal framework allowing to

reconcile sanitary efficiency and protection of citizens' public liberties. In this opinion, the authority sets out the essential principles that make the TousAntiCovid application "GDPR-compatible", [9] thus making it possible to anticipate constraints. Beyond that, because fears for fundamental freedoms are great, it also questions the appropriateness of such a system. Going back to basics. To get out of the controversy linked to the debate on the infringement of individual liberties, which certainly exists but is nevertheless limited here, it is important to return to the fundamentals. The lawfulness of such a system will therefore depend on the purpose and legal basis of the processing.

4.1 Overview of how TousAntiCovid application works in collecting data

4.1.1 Volunteering as a legal basis

The installation of TousAntiCovid applications based on consent or voluntary action. As the law stands in respect of rights and freedom, monitoring should be carried out on a voluntary basis by the persons concerned. The system must be designed in such a way to allow users to have control over their data. [10] This consent also must validate within the meaning of the GDPR, i.e., it must be informed, in other words, preceded by precise, purpose-specific, unambiguous, and free information: a refusal to consent must therefore not expose the person to any consequences whatsoever. This must be considered because international comparisons show that volunteering sometimes has as a counterpart a limitation of freedoms. In the absence of real consent, a law containing important safeguards would be necessary.

4.2 Data Access and Information Structure

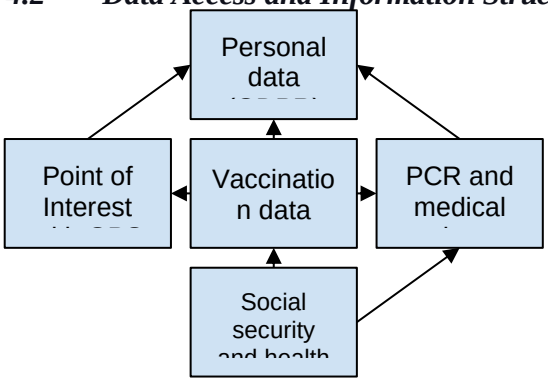

Figure 1. Information structure of tracing application in France

Figure 1 illustrates information structure if tracing user information related to the covid19 outbreaks. It is mainly concerned about which places a person has visited. To enter Point of Interest, visitors need to show a pass sanitaire that proves that they have been fully vaccinated. From a user point of view, we never show our personal data to any entity. The important role of GDPR in this case is to protect personal data and make sure the information about tracking details will not be used for other objectives and not used by third parties. The main utilization of the data is to know the human mobility related to the covid19 outbreaks. When a patient is detected positive of covid they will know for two weeks this person went to which point of interest and group the potential interaction around the places to detect and trace the possible contamination.

This invocation of voluntariness is thus open to question. Indeed, the freedom to consent is largely biased, whether because of social pressure, fear of illness, or the fact that abusive behaviour could lead to people being asked to justify the installation of the application to gain access to a place. The *Comité Consultatif National d'éthique* (CCNE) [11] thus states in its recommendations, in the case of voluntary monitoring, free adherence would be encouraged by informing the public about the usefulness of monitoring and by appealing to a sense of civic responsibility, social encouragement, for example by sending SMS and public messages which suggests that pressure will be put on individuals. [12] Obtaining informed consent is also difficult. Indeed, individuals still need to be fully able to appreciate what they are consenting to, whether consent to the processing of location data, consent to the processing of other information, including health data, or the level of confidentiality and security offered by the technology used, the subsequent communications in the event of a report sent or alert received, and the risks identified in the data protection impact assessment. All these uncertainties about consent should lead to its removal as a legal basis to be anchored in the law to ensure its temporary nature and set out the guarantees to be implemented and appropriate controls. The CNIL thus considers that the pursuit of a public interest mission to combat the Covid-19 epidemic constitutes a more appropriate legal basis than consent, which implies having a sufficient legal basis in a norm of national law. Pursuant to the GDPR, this processing is provided for by national or Union law and that it provides for appropriate and specific measures to safeguard the rights and freedoms of the person concerned. [13] Clearly, the installation of an application which is intended to enable alerts to be made (to report oneself as a carrier of Covid-19 with the possible consequence of a quarantine decision, to report to third parties that they have been in contact with an infected person) is part of the pursuit of a public health objective, or even in the context of a state of public health or public safety emergency.

The idea that data processing should proceed on terms other than consent simply does not undermine the principle of voluntariness. Voluntariness could be one of the safeguards provided for by the legislator. The responsibility of the public authorities in its implementation (choice of technology, impact assessment, ex-post control) would therefore also have its full effect. The choice of relying on consent is also questionable since it has the consequence of ruling out

any precise framework by the legislator, as well as the ensuing legality control. Contrary to what seems to be claimed, consent does not provide any guarantees. It has the effect of impoverishing the guarantees that may be offered. This focus on consent perfectly illustrates the great misunderstanding about the role and purpose of consent in personal data protection legislation. Installing an application does not make it possible to express consent to the underlying processing, nor does consent to location, by activating the location option. Furthermore, the legal basis for the processing cannot be consent. Indeed, the health context may not allow the conditions for consent to be met. [14] Moreover, the basis for consent would weaken the solution because of the associated right of withdrawal. Nevertheless, voluntary action at the initiative of the use of the application must be clearly distinguished from it as an element of acceptability and trust. There may be a willingness to install the application without consent constitutes the legal basis for the processing of the data thus collected by the application within the meaning of the GDPR. Two bases could then make the processing lawful. The first, general, is referred to in Article 6(1)(e) of the GDPR, which refers to the performance of a public service mission. The second, specified in Article 9(2)(i) and specific to health data, authorises their processing by way of derogation for reasons of public interest in the field of public health, such as the protection against serious cross-border threats to health. In any event, the solution should be based on national legislation and should necessarily be exceptional, thus limiting its use in time and, consequently, the retention of the data processed in this way. The recognition of a legal basis is not enough. As the *Commission Nationale de l'Informatique et des Libertés* (CNIL) reminds us, it will be essential to respect all the principles of the GDPR and the rights enshrined therein, as well as to ensure a sufficient level of guarantees, particularly in terms of security, insofar as the technological solution is likely to infringe fundamental rights and freedoms.

4.1.2 Emphasis the anonymity and pseudonymity

The GDPR introduces a new concept in European data protection law, pseudonymisation to protect individuals' rights yet allow data controllers the usefulness of the data. [15] Pseudonymisation can strengthen privacy protection by replacing the majority of identifying fields within data records with a unique or multiple data identifier or alias. This method is subject to technical measures to ensure that the data collected remains anonymous. The GDPR requires technical and organisational measures to ensure that no attribution or non-attribution is made to an identified or identifiable person. However, the GDPR does not apply to anonymised information. Pseudonymisation is not the same as anonymisation. However, both pseudonymisation and anonymisation are used to protect the privacy rights of data subjects and permit organisations to balance their privacy rights with its legitimate purposes. [16] The so-called pseudonymisation of data refers to the processing of personal data by replacing any identifying characteristics of the data with a pseudonym, whereby the data defies direct attribution to a natural person without the use of additional information. This process of pseudonymisation has a lower power density compared to the process of anonymisation, which attempts to prevent the possibility of identifying completely and irreversibly an individual. Pseudonymisation replaces only part of the data. For example, a person is given a new name, address, and date of birth. Compared to anonymised data, this information is nevertheless classified as personal and therefore subject to the GDPR. The harms and repercussions of a pseudonymised data breach are, however, less significant.

The alias is a key safeguard for the processing of personal data for scientific, historical, and statistical purposes. However, Article 89(1) requires that data protection during processing activities is ensured by the application of appropriate technical and organisational measures under this Regulation, for safeguarding the rights about the privacy of the data subject [17]. These measures apply to the determination of the processing method and to the execution of the processing activities. Organisational and technical security measures include encryption, confidentiality and pseudonymisation of confidentiality, integrity, and resilience, together with conventional testing processes. As part of a privacy by design strategy, organisations may wish to use anonymisation or pseudonymisation techniques to provide better protection for data subjects. Pseudonymisation involves separating data from their respective owners and making it impossible to link them to identity without additional information. In short, it is a privacy-enhancing technique where directly identifying data is kept separate and secure from the processed data to ensure non-attribution. Consequently, under pseudonymisation, data is not entirely anonymous without being identifiable. Through the GDPR, controllers were urged to adopt codes of conduct that are approved by Member States, supervisory authorities, the EDPB or the Commission. The concept of a code of conduct introduced by the GDPR would be a novelty compared to the French law of 1978, even if occasional actions by the CNIL in recent years were already part of a similar approach. At the European Union level, the concept of a code of conduct is introduced by Directive 2005/29/EC concerning unfair business-to-consumer commercial practices in the internal market. This directive defines the code of conduct as an agreement or series of rules not imposed by the legislative, regulatory, or administrative provisions of a Member State stipulating the behaviour of professionals who undertake a commitment binding on them in terms of one or more commercial practices or one or more sectors of the commercial activity [18].

The GDPR does not apply to anonymous data processing, i.e. information that cannot or can no longer be linked to an identified or identifiable natural person. The analysis of people's movement flows based on anonymous or anonymised data is therefore perfectly feasible. However, anonymity is undetermined. It is not enough to depersonalise data (i.e. remove identifiers or replace them with pseudonyms or coded data) to consider the data anonymous, it must be possible to demonstrate that there is no re-identification or re-attribution of the data. The tracing of pedestrian flows using Wifi technology was thus considered not to have the required anonymity insofar as it was a question of following the movements of the same individual over time. For the data protection authorities, to be able to consider that a processing operation is anonymous, three conditions must be met: unable to singularise the data of an individual, unable to link the data to those of a given individual, and unable to deduce or infer information about an individual. Compliance to these three conditions, generally implying the aggregation of data or even the introduction of random data. There are no technical references, standards, or labels to validate the effectiveness of the anonymisation processes. Moreover, the fact that data may initially be collected anonymously does not guarantee that the processing will be anonymous from the beginning to the end. Thus, before qualifying a processing operation as anonymous, all the stages of the processing operation must be considered. The fact that one of the functions of the processing is to allow individual, as well as the fact that the data can be reused and linked with other data for various studies or analyses related to the fight against the Covid-19 pandemic, must be duly considered in assessing the risk of re-identification or re-allocation. Given these simple considerations, it is doubtful whether the system can be fully deployed anonymously. The use of pseudonymisation or anonymisation mechanisms is undoubtedly one of the strong guarantees that can be offered to avoid misuse, but it is not sufficient, even coupled with 'voluntariness', to remove all doubts.

4.2 Limitations provided under the GDPR

4.2.1 Specific requirements for the processing of sensitive data

The GDPR's Article 23(1) offers several restrictions on application of the regulation designed to secure public security or other significant public interest objectives like public health. The article entitles Member States from restricting the rights of data subjects and important data protection principles by legislative measure. Such legislation respects the essence of fundamental rights and freedoms and constitutes necessary and proportionate measures in a democratic society [19] In this sense, Article 67 of the French Data Protection Act (FDPA) foresees a specific derogatory regime for the processing of personal data in the field of health care. This derogatory regime, which is justified by the urgency of the matter, ends one year after the treatment has been put in place and the sole purpose of the processing is to respond to a health alert and to manage the consequences. Nonetheless, this does not mean that such treatments could be implemented without a precise framework. The implementation of measures to guarantee public health can only take place within the framework of a strict proportionality check concerning the health risks incurred and the circumstances of time and place and must be terminated without delay when they are no longer necessary [20], as these requirements apply de facto to the underlying processing of personal data. One of the consequences of an interpretation that seeks to exclude the application of Union law would probably be to allow a more flexible application of the proportionality check. [21] Furthermore, the general provisions of the FDPA remain applicable to such processing whether it is subject to the GDPR. Also, the application of the general principles of data protection to the processing of personal data in connection with the Covid-19 pandemic, which it is appropriate to present now, must be done considering the existence of this context.

4.2.2 Very limited scope for consent

Consent is not a legal basis for the processing of personal data in the context of the Covid-19 epidemic. [22] The very demanding interpretation of these conditions by the data protection authorities only makes consent admissible as a legal basis to operate the TousAntiCovid application or exemption to the prohibition on processing sensitive data. It provided that the data subject has genuine freedom of choice and can refuse to give it without prejudicial consequences. These conditions may appear difficult to respect in the context of processing operations linked to the Covid-19. Indeed, consent cannot be invoked if the refusal results in the impossibility of access to a service in the stigmatisation or different treatment of the person (for example access to medical care or treatment or access to premises). Since consent is unconsidered free in the presence of elements of coercion or pressure, thus, when the controller is a public authority, the imbalance is presumed, insofar as the data subject will have no realistic alternative to accepting not only the processing but also the conditions of their personal data processing. [23]

The implementation TousAntiCovid respects the principles of the GDPR: proportionality, transparency, and legality. [24] By virtue of Deliberation No. 2020-056 of 25 May 2020, the CNIL notes that the guarantees taken by the government have considered its previous Deliberation No. 2020-046 of 24 April 2020, about the fact that the application must be voluntary. It also specifies that the system complies with the necessity and proportionality required by the GDPR while making a few observations that will have to be verified as the application is rolled out. The EDPB recalled that the legality of location tracking devices in France and elsewhere depends on compliance with the GDPR and

the e-Privacy Directive. Consequently, processing of location data can only occur if the data is anonymised or with the consent of the data subjects. The EDPB underlines a preference for the least intrusive solutions and that health emergency measures must respect the Charter of Fundamental Rights and the ECHR. Article 2 of Decree No. 2020-650 [25] specifies in this respect that the data are pseudonymised: the data subject receives a randomly generated unique identifier and a random and temporary pseudonym that is renewed every day when the application is downloaded.

4.2.3 Processing of health data by private sector

The possibility for private organisations (employers, insurers, etc.) to process sensitive data in relation to the Covid-19 pandemic, including health data, is also minimal. The GDPR's Recital 54 states that processing of health data for reasons of public interest may not imply the processing of personal data for other purposes by third parties to be processed, such as employers or insurance companies and banks. Nonetheless the GDPR does provide an exception for health data processing necessary to comply with the obligations or exercise the rights of the controller or data subject in the field of employment law, social security, and social protection. As in the case of public authorities, consent can be difficult to invoke and is assumed to be unfree, due to the subordination relationship or to the fact that it is impossible to refuse consent with not de jure or de facto prejudicial consequences (e.g. in the context of the processing of applications for supplementary health insurance). Analysing the conditions of legality therefore leads to the conclusion that pandemic Covid-19 personal data processing operations require statutory provision and pursue public interest or public authority purposes, especially when health-related data are involved. Data processing activities undertaken outside the scope of the Directive comply with certain other conditions of lawfulness laid down in the legislation on the protection of personal data and primarily with the principles of purpose and minimisation. It is essential to seek a balance between the objective of health efficiency through an application that allows people to be tracked while simultaneously ensuring the protection of privacy. Also, a limit on the length of time that data can be kept should be set. Article 3 of Decree No. 2020-650 thus limits the retention period to six months after the end of the state of a health emergency. According to the President of the CNIL, “it is also preferable to give priority to storing data locally, on the user's terminal, where possible. Applications based on Bluetooth data, which are encrypted directly on the phone under the control of the user, provide more guarantees than those based on continuous geolocalized tracking (GPS) of people ". Article 2 of decree no. 2020-650 chose to store the data either on a central server, on the user's terminal or shared on both devices. Bluetooth technology was also chosen. The CCNE, which was asked to examine ethical issues related to the design, implementation and use of digital tools, issued a report containing numerous recommendations. It came out in favour of the interoperability of tracing applications on a European scale in compliance with the GDPR. It insists on the need to choose technical means of proximity detection that promote the protection of privacy and personal data or to submit tracing applications to audit by trusted third parties.

5. CONCLUSION

Numerous services in the digital environment necessitate personal data in order to work properly. Internet users, for example, receive multiple requests for terms and conditions every day requiring clicks and swipes to respond. As a result, individuals lack full awareness of how their personal data is collected, prepared, stored and used. This situation has led to a lack of anticipation and awareness in public. Some stakeholders are increasingly using their personal data in ways that include making and obtaining personal data. In the situation of the Pandemic as a society that obeys the policies made by the government, it seems as though there is no other choice except to abide by the existing rules. As the CNIL points out, it will be essential to respect all the principles of the GDPR and the rights enshrined in it. Equally, it is essential to ensure a sufficient level of safeguards, especially in terms of security, as the technological solution is likely to affect fundamental rights and freedoms. Although the principle of personal tracing must be socially and ethically adopted a precise and demanding roadmap for its application is indispensable. The roadmap ought to include a redefinition of the role of voluntary action to identify a suitable legal basis.

REFERENCES

[1] World Health Organization, *Contact Tracing in the Context of Covid-19*, 10 May 2020, [online], https://www.who.int/publications/i/item/contact-tracing-in-the-context-of-covid-19 (accessed 28 October 2020).

[2] Ministry of Communication and Information Technology of the Republic of Indonesia, *Apa itu PeduliLindungi*, [online], https://pedulilindungi.id/#tentang (accessed 28 October 2020).

[3] France Government, *Info coronavirus Covid-19 – Application Tousanticovid*, [online], https://www.gouvernement.fr/info-coronavirus/tousanticovid (accessed 28 October 2020).

[4] European Data Protection Board, *Statement by the EDPB Chair on the Processing of Personal Data in the Context of the Covid-19 outbreak*, 16 March 2020, [online], https://edpb.europa.eu/news/news/2020/statement-edpb-chair-processing-personal-data-context-

covid-19-outbreak_fr (accessed 28 October 2020).
[5] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).
[6] Cécile Crichton, StopCovid: parution du décret portant création de l'application", 04 Juin 2020, *Dalloz Actualite*.
[7] Tom R. Tyler, "Methodology in Legal Research", Utrecht Law Review, Volume 13, Issue 3, 2017.
[8] Code de procédure pénale Chapitre V – de la Géolocalisation (La loi n° 2014-372 du 28 mars 2014, article 1).
[9] Alexandra Bensamoun, Nathalie Martial-Braz, "Covid-19 (déconfinement) : avis de la CNIL sur l'application StopCovid", *Recueil Dalloz*, 2020, p.934.
[10] GDPR Article 6.1.a and FDPA Article 5.1.a (with the exception of cases where the processing data is not covered by the GDPR).
[11] The *Comité Consultatif National d'Ethique* is a French governmental advisory council on bioethics issues.
[12] CCNE, *Bulletin de veille No.1*, 07 April 2020, p.11.
[13] GDPR Article 9.2.i
[14] GDPR Article 4.11, 7 and 9.2.a
[15] Arnaud Lecourt, "RGPD : nouvelles contraintes, nouvelles strategies pour les entrepises", *Dalloz IP/IT 2019.* 205
[16] Thierry Bonneau, "L'accès aux données bancaires au regard du respect de la vie privée", *Lexis 360, Revue de Droit bancaire et financier*, N° 6, Novembre 2018, dossier 39, p.5.
[17] The FDPA has seized the margin of manoeuvre opened by Article 89 of the GDPR and offers all these treatments necessary derogations from the rights of the persons concerned. Lucie Cluzel-Métayer, Émilie Debaets, "Le droit de la protection des données personnelles : la loi du 20 Juin 2018", *RFDA 2018*, p.1101.
[18] See Javier Lete, "La publicité à la lumière de la jurisprudence de la Cour de justice de l'Union européenne", *Rev.UE 2015*, p. 468.
[19] The Charter of Fundamental Rights of the European Union, Article 52.1 and the European Convention on Human Righs, Article 8.2, which list among the legitimate objectives that may justify infringements of the right to the respect for private and family life: public security or the economic well-being of the country, the protection of health or the protection of the rights and freedoms of others.
[20] Code de la santé publique, article L3131-15
[21] GDPR article 6 as translated in article 5 of FDPA.
[22] GDPR Article 4.11
[23] Working Party 29 (WP29), Consent Guidelines, p.7
[24] A. Guérin François, "Coronavirus: les recommandations du Comité européen de la protection des données aux responsables de traitements", *Dalloz Actualité*, 30 March 2020 ; D. Ventura, "Coronavirus et suivi de localisation : le Comité européen de la protection des données en première ligne", *Dalloz Actualité*, 10 Avril 2020.
[25] Decree No. 2020-650 issued on 29 May 2020 relating to data processing known as "StopCovid".