MEMO-P3007
Raban OHLHOFF
00457528
05.2020

OPEN SOURCE OU *PROPRIETARY CODE* DANS LES *SMART CITIES*

TABLE DES MATIÈRES

INTRODUCTION

Cette analyse a comme objectif d'observer et d'évaluer différents concepts de systèmes développés pour la gestion du réseau de la *smart city*. La comparaison sera effectuée entre des systèmes distribués et développés sous une licence *open source* et un système de gestion et d'évaluation distribué sous une licence propriétaire. Il s'agit de mener des recherches sur des exemples concrets en décodifiant leur fonctionnement technique. Leurs modes de fonctionnement respectifs sont sujets d'une évaluation concernant le respect du droit à la vie privée.
Au premier lieu il est nécessaire de concentrer la recherche sur deux exemples venants de deux champs opposés par leur degré de liberté d'accès à leur code source. L'exemple le plus propice pour représenter les solutions qui viennent du champ des logiciels open source est le projet *FIWARE* [1]. Avec sa documentation abondante et l'implication événementielle, une analyse des approches poursuivie par ce projet peut mener à une compréhension générale du mode de fonctionnement des logiciels avec un code source accessible.
Le projet *FIWARE* inclut une multitude de projets partageant le même code comme *FIWOO* [2] et d'autres projets utilisant les API développés par la communauté [3].
Le projet de l'*Alibaba group*, nommé *City brain* [4], sera étudié comme représentation exemplaire d'un système distribué sous licence propriétaire et non accessible par le publique. Alibaba cloud dispose également d'une documentation bien fournie au sujet de leur *smart city solution* [5]. Il sera néanmoins plus difficile d'obtenir des informations indépendantes car il est impossible de vérifier les informations indiquées par leur équipe marketing parce que une vérification dans leur code source n'est pas donnée, bien évidemment. Il s'agit donc dans cet exemple de trouver des informations fiables sur leur projet *city brain* et plus concrètement sur leurs systèmes de traitement de données récoltées. Les deux réseaux sont étudiés en requestionnant les manières d'interagir avec les données personnelles et à évaluer le degré de protection de celles-ci.
Ces évaluations sont suivies par une conclusion sur les avantages et risques des systèmes au niveau du droit fondamental.

HYPOTHÈSE

La recherche est axée autour d'une comparaison de deux systèmes différents et leurs méthodes d'interagir avec les informations personnelles des habitants de la ville. Est-ce qu'un code accessible et visible par la population diminue le risque

[1] https://www.fiware.org [2] https://www.fiwoo.eu [3] https://www.fiware4water.eu ; https://synchronicity-iot.eu/ https://autopilot-project.eu/ ; https://www.iof2020.eu [4] https://www.alibabacloud.com/solutions/intelligence-brain/city [5] https://www.alibabacloud.com/help?spm=a2c63.m28257.3156523820.dnavdocumentation0.18b55922wgv639

d‘une utilisation des données privées à des fins qui soient en contradiction avec le droit à la vie privée ? On peut également requestionner une ouverture du code qui pourrait éventuellement faciliter la création des logiciels malveillants interceptant le transfert des donnés. Qui ou quelle institution régule la gestion et la manière d’interagir avec ces données ? Lesquels des deux systèmes est le plus favorable dans le contexte d’une protection des informations personnelles ? En général, les questions ici concernent le degré de sécurité des transferts mais également du stockage et de l’utilisation des données personnelles.

MÉTHODIQUE

L’analyse commence avec une définition du droit fondamental à la vie privée, et son rôle dans la société contemporaine. Il ne s’agit pas de définir les droits selon des critères juridiques écrits dans la charte de chaque pays mais plutôt d’en abstraire les notions pour définir le concept d’une manière mondiale. C’est à dire que nous nous concentrons sur les valeurs fondamentales que ce droit représente et protège. Après avoir étudié la signification de la notion de vie privée, nous analysons les systèmes *FIWARE* et *City Brain* selon les valeurs représentées par le droit fondamental et leurs modes de fonctionnement concernant ces questions sociétales. Les deux cas concrets servent d’exemples pour représenter les deux approches dominantes dans le développement technologique : le *FLOSS* [6] et le développement commercial [7]. La partie d’analyse du logiciel open source tente d’expliquer d’abord le fonctionnement général de la plateforme et ensuite de rentrer dans les mécanismes sécuritaires et ses limitations. Dans la deuxième partie, l’exemple *closed source* est brièvement introduit et puis étudié sous l’angle de la protection des données privées. L‘intention ici est d‘évaluer les deux différents concepts selon des critères objectifs et comparables. C’est à dire que leurs modes de fonctionnement sont abstraits à un certain degré pour aboutir à des résultats comparables. Cette étape est suivie d’une conclusion sur l’évaluation traitée dans l’analyse et des réponses aux hypothèses de recherche sont proposées.

ÉTAT DE L‘ART

Des documents faisant des comparaisons générales entre les *FLOSS* et les logiciels propriétaires sont nombreux. Par exemple les articles sur le blog de *Sam Saltis* [8]

[6] https://www.gnu.org/philosophy/floss-and-foss.de.html [7] https://www.sec.gov/Archives/edgar/data/1124804/000119312508212359/dex104.htm [8] SALTIS, M. 2020. « Comparing Open Source Software vs Closed Source Software », *Coredna*, https://www.coredna.com/blogs/comparing-open-closed-source-software

ou bien l'article publié sur *Govtech* [9]. Mais dans ce contexte, une comparaison des différentes manières de traitement d'informations est plus pertinente. Il existe un certain nombre d'études qui ont été publiées ces dernières années dans le domaine de la recherche sur l'emploi des technologies *open source* pour une ville intelligente. On trouve notamment des recherches qui ont été faites en observant la méthode du système *FIWARE*. Pour ce sujet, l'article publié par *Peter Detzner* [10] et *Peter Salhofer* [11] s'avère fournir des informations suffisamment complètes pour comprendre le fonctionnement. Un travail fournissant des informations concernant les mécanismes sécuritaires du logiciel est publié par *Flavio Cirillo* et al. [12]. La documentation par la *FIWARE foundation* et leur repositoire du code se sont également avérés utiles [13;14].
En ce qui concerne une analyse du système *closed source* qui est le *City brain* de *Alibaba group,* les recherches sont moins abondantes. La source la plus adéquate était rédigée par *Xian-Sheng Hua* et al., sous la direction du groupe *Alibaba* [15]. Des sources scientifiques indépendantes sont difficilement trouvables [16]. Ensuite au sujet de l'interaction entre les individus et ces systèmes de gestion d'information, il existe des études sur le respect du droit à la vie privée, entre autres, par *Isaac Potoczny-Jones* et al. [17], dans la publication de *Nasser H. Abosaq* [18], l'étude menée par *Adel S. Elmaghraby* [19] ou encore le travail de *Raj Gaire* et al. [20]. Ce travail tente à apporter une contribution à l'état de la recherche en faisant l'analyse et la comparaison des exemples populaires venants des deux champs, sous l'angle du droit à la vie privée.

DROIT À LA VIE PRIVÉE

Avec le progrès récent des technologies intelligentes, il s'est développée une tendance à rendre la ville plus rationnelle et plus performante grâce à l'emploi des senseurs divers, collectant des informations sur différents champs. Ses données ne concernent pas uniquement la ville en tant qu'objet, mais regardent dans la majorité des cas l'interaction entre les habitants et leur environnement. À l'aide de ces données, des simulations et par cela des prédictions sur le comportement

---

[9] COLLINS, H. 2009. « Is Open Source Software More Secure than Proprietary Products? », *Govtech*, https://www.govtech.com/security/Is-Open-Source-Software-More-Secure.html [10] DETZNER, P. ; SALHOFER, P. 2020. *Proceedings of the 53rd Hawaii International Conference on System Sciences,* Analysing FIWARE's Platform - Potential Improvements, Frauenhofer Institut Dortmund [11] SALHOFER, P. 2018. *Proceedings of the 51st Hawaii International Conference on System Sciences,* Evaluating the FIWARE Platform, FH Joanneum [12] CIRILLO, F. *et al*. 2019. *A Standard-based Open Source IoT Platform: FIWARE*, Heidelberg, NEC Laboratories Europe. [13] http://forge.fiware.org/plugins/mediawiki/wiki/fiware/index.php/Main_Page [14] https://github.com/Fiware [15] HUA, X. *et al.* 2019. *The City Brain: Practice of Large-Scale Artificial Intelligence in the Real World,* Hangzhou, IET Research Journals. [16] BEALL, A. 2018 « In China, Alibaba's data-hungry AI is controlling (and watching) cities », *Wired* , https://www.wired.co.uk/article/alibaba-city-brain-artificial-intelligence-china-kuala-lumpur [17] POTOCZNY-JONES, I. *et al.* 2019. *Encrypted Dataset Collaboration,* Portland, Association for Computing Machinery. [18] ABOSAQ, N. 2019. *Impact of Privacy Issues on Smart City Services in a Model Smart City,* Yanbu, Yanbu University College. [19] ELMAGHRABY, A. 2013. *SECURITY AND PRIVACY IN THE SMART CITY,* Ajman, AIUPC. [20] GAIRE, R. *et al.* 2018. *Crowdsensing and privacy in smart city applications*, Canberra, CSIRO.

peuvent être établies. Grâce à des nouvelles technologies comme l'intelligence artificielle [21], les modèles peuvent être optimisés de manière autonome. Mais cela nécessite l'entrée des *big/mass data* [22] pour permettre aux logiciels de proposer des optimisations. Ces données peuvent être directes ou indirectes, anonymes ou personnelles. Cette collection de bases de données et leur évaluation par les systèmes pose des questions urgentes à l'égard de la protection de la vie privée des individus concernés.
La notion de vie privée suggère l'existence du contraire : une vie 'publique' nommée *état civil* [23]. La limite entre les deux n'est pas toujours claire et dépend fortement d'une définition individuelle selon des valeurs personnelles. Certaines personnes décident de partager des informations sur leurs vies avec le publique. Dans ces cas, ces données changent du domaine du privé au public et ne sont plus à considérer comme étant de l'ordre privé dans le sens propre. Mais qu'en est-il des informations personnelles qui sont recueillies contre le grès des individus ? À ce moment-là il s'agit d'une infraction du droit à la vie privée qui devrait être prohibée par la législation des états. Pour pouvoir évaluer à quel moment il s'agit d'une violation de la protection des données personnelles, il faut définir quels domaines sont compris dans cette notion:
En général, il s'agit de toutes les informations qui ne concernent ni le publique, ni la collectivité et qui sont par cela individuelles. Elles sont à protéger à tout prix car elles peuvent être sensibles et risquent d'exposer la personne concernée au public quand elles deviennent accessibles par des tierces personnes. Les données privées peuvent être entre autre: des valeurs, des émotions, des avis, des intérêts, des préférences ou bien des informations physiques comme le trajet habituel, l'état de santé ou encore la routine quotidienne.
La décision de partager ces informations en dehors du cadre intime doit être libre à chaque individu. Il y a néanmoins des exceptions à cette règle dans la réalité. Quand il s'agit de recueillir des informations personnelles de certains groupes de personnes pour mieux pouvoir protéger un plus grand nombre d'individus, l'activité des agences de sécurité nationale par exemple, la limite commence à devenir floue. Dans les chapitres suivants, les deux cas concrets sont expliqués, étudiés et ensuite comparés et il sera montré que *FIWARE* est plus favorable concernant la protection des données privées.

[21] TEGMARK, M. s.a. « BENEFITS & RISKS OF ARTIFICIAL INTELLIGENCE », *future of life institute*, https://futureoflife.org/background/benefits-risks-of-artificial-intelligence [22] RADTKE, M. 2019 « Was ist Big Data ? », *Bigdata insider*, https://www.bigdata-insider.de/was-ist-big-data-a-562440
[23] https://fr.wikipedia.org/wiki/%C3%89tat_civil

DROIT À LA VIE PRIVÉE - *FIWARE*

Avant de commencer à étudier les mécanismes de protection ou des éventuelles défaillances au niveau de la protection des données personnelles dans le système *FIWARE* il faut comprendre l'architecture interne du logiciel.
Il s'agit d'un projet fondé en 2011 à la suite des initiatives de part de l'union européenne comme le *Seventh Framework Programme* [24] avec un budget de 70 millions d'euros. Bien que *FIWARE* soit entièrement open source et à but non lucrative sans intervention commerciale, le développement est fortement maintenu par l'organisation *FIWARE foundation* [25] qui reçoit des fonds de la *commission européenne* consacrés au progrès dans le développement de cette plateforme *IoT.*
La plateforme se compose de plusieurs différents composants (*APIs* [26]) qui remplissent chacun des fonctions différentes. Le projet se trouve en constant progrès et des nouveaux *APIs* se voient rajoutés régulièrement au projet principal. L'avantage de l'accessibilité au code source des composants est la standardisation, qui permet une meilleure intégration des nouvelles technologies dans le réseau de cette plateforme [27]. Le composant principal est le *Context broker* nommé *ORION* [28] qui remplit le rôle de mémoire de l'état de l'application, stockée dans une base de données *Mongo NoSQL* intégrée dans le module via un protocole *NGSI* [27]. *ORION* informe également les autres composants d'un éventuel changement des valeurs. Chaque interaction (*fiware-service* [27]) est séparée dans un processus indépendant des autres et a un accès uniquement sur les données prévues pour ce service. Le deuxième composant essentiel pour le réseau est le *IDAS* [28] qui sert d'interface entre les senseurs et les autres *APIs*. Les derniers modules qui complètent le réseau sont appelés *CYGNUS* et *COMET* [29]. Ils jouent le rôle de stockage pour des valeurs historiques. Tous ces outils interagissent entre eux via le protocole *HTTP REST* [30] mais les données ne sont pas encore sécurisées à ce moment-là.
La protection des données se manifeste au moment d'un accès extérieur à celles-ci. Chaque flux d'information entrant ou sortant de la plateforme passe par un mécanisme d'authentification appelé *OAuth2 protocol* [30]. Ce protocole se compose de trois sous-composants qui sont le *identity Manager* (*IdM*), le *Policy inforsement Point* (*PEP*) et *AuthZForce* [30].
Le moment de la réception d'une demande de lecture d'une certaine valeur, le *PEP* vérifie si l'utilisateur dispose d'une autorisation pour lire cette valeur spécifique. Ces autorisations sont stockées par le *AuthZForce* et sont liées avec le compte d'utilisateur créé et enregistrées par l'*Identity manager*. Pour faciliter la

[24] https://ec.europa.eu/research/fp7/index_en.cfm [25] https://www.fiware.org/foundation/ [26] https://www.redhat.com/de/topics/api/what-are-application-programming-interfaces
[27] DETZNER, P. ; SALHOFER, P., *op.cit*., p.6609. [28] https://github.com/telefonicaid/fiware-orion [29] DETZNER, P. ; SALHOFER, P., *op.cit*., p.6610. [30] DETZNER, P. ; SALHOFER, P., *op.cit*., p.6611.

compréhension de ce fonctionnement, on peut s'imaginer que chaque utilisateur doit disposer d'un compte qui est caractérisé par différentes autorisations. Ce processus permet une régulation optimale des accès selon les différents utilisateurs. Une fois la vérification des autorisations validée, la valeur demandée sera rendue accessible pour l'utilisateur via un proxy sécurisé par le *PEP* [29]. Cela veut dire qu'une personne ou un logiciel extérieur n'as uniquement accès aux données pour lesquelles il est autorisé et il n'y aurait dans aucun cas une interaction directe entre une tierce personne et les bases de données stockées dans le serveur.
Dans la théorie, les données, personnelles ou pas, se trouvent parfaitement verrouillées de tout accès abusif. Mais comme chaque système il se trouve qu'il y a des défaillances difficilement solubles. Le problème principal, c'est qu'aucun système n'est entièrement protégé par la couche de protection virtuelle car il se trouve toujours objectivé dans le monde non-virtuel. Les bases de données se trouvent sur des serveurs dans des bâtiments spécialisés et sont donc relativement bien protégées physiquement mais les senseurs qui registrent différentes sources se trouvent, dans la majorité des cas, exposés au public sans contrôle intensif possible. Une interception des données avant qu'elles arrivent dans le réseau protégé de la plateforme est donc difficilement évitable. Le même problème se trouve chez l'utilisateur à l'opposé de la chaîne. Une *malware* qui s'introduit dans le médium de l'affichage des données, pourrait dans le cas échéant espionner des données [31].
Un deuxième problème consiste à la maintenance du système et la distribution des autorisations. Le fonctionnement de la plateforme implique obligatoirement une instance qui évalue quels droits d'accès sont à distribuer à quel utilisateur et dispose par cela des droits administrateurs sur la plateforme et de leurs données. Il y'aura donc toujours une personne qui dispose des droits supérieurs aux autres et du libre accès aux données privées.

DROIT À LA VIE PRIVÉE – *CITY BRAIN*

Contrairement aux travaux publiés sur *FIWARE*, il n'existe qu'un nombre limité de travaux de recherche menés sur *City Brain*, ce qui complique l'évaluation du concept sécuritaire du logiciel. De plus, la source la plus complète est éditée sous la commande de *Alibaba Group* [32] et n'est donc pas à considérer comme référence indépendante. Elle sert néanmoins d'outil pour mieux comprendre la plateforme qui se trouve étant différente dans plusieurs points comparés à l'exemple étudié dans

[31] FISCHL, G. 2020. « Mandrake: Android-Schädling stiehlt Daten seit 2016 », *Connect*, https://www.connect.de/news/mandrake-android-malware-stiehlt-daten-apps-play-store-3200783.html [32] HUA, X. *et al., op.cit.*

le chapitre précédant.
City Brain a vu le jours en 2016 dans le cadre d'une recherche sur l'optimisation de la circulation routière à l'aide d'une intelligence artificielle [33]. Les champs d'application s'élargissent au fur et à mesure pour proposer une application dans une multitude des domaines.
Aujourd'hui l'*IA* se voit intensivement utilisée dans de nombreuses villes en Chine [34] mais également en dehors des frontières chinoises. Le logiciel propose une *end-to-end solution* en faisant des analyses de différentes manières sur des *big datas* recueillies par les senseurs et cameras dispersés dans la ville. Si dans *FIWARE* la partie d'évaluation et prédiction des donnés par du *machine learning* était un composant facultatif, dans *City Brain* elles constituent l'élément crucial du système. En effet le système fonctionne à l'aide de reconnaissance d'images, d'exploration de données et d'apprentissage automatique appliqués aux blocs de *big data* composés d'informations sur la ville et ses habitants [35]. Les champs d'applications actuelles revendiqués par les développeurs sont l'analyse de l'infrastructure urbaine, la surveillance policière automatisée, l'évaluation de la circulation urbaine, les optimisations des trajets et la proposition d'aménagement urbain automatisé [36]. Le système fonctionne en trois étapes principales [35] qui sont d'abord le recueillement des données et une première analyse de ceux-ci pour les catégoriser (cognition). Ensuite il s'agit de l'étape de la décision et d'optimisation calculée par *City Brain* pour enfin arriver à la phase de la prédiction. Chacune des étapes est problématique au niveau du respect des droit fondamentaux des habitants, ce qui sera évalué dans le chapitre suivant. Faute d'informations plus détaillées du fonctionnement de l'*IA* et plus concrètement sur les caractéristiques de l'algorithme décisive ou prédictive il faut se concentrer sur l'analyse des données qui entrent dans le système.
Les sources principales alimentant le logiciel sont des caméras placées dans l'entièreté de la ville [37] mais les flux d'informations entrants peuvent être augmentés par des signales *MAC*, des micro-ondes, *GPS*, signales *RFID* et des informations personnelles sur les réseaux sociaux. À base de ses données, le logiciel développe les algorithmes de décisions, d'optimisation et de prédiction [38]. Le logiciel est également capable de *person re-identification* (*ReID* [39]) ce qui consiste en développant une base de données individuelles pour chaque habitant à base des informations recueillies. Ces Informations d'identification sont utilisées entre-autre pour faciliter le travail policier, pour retrouver des criminels fugitifs ou prédire des probabilités par zones, nécessitant une intervention policière [36]. Le sujet de protection des données privées n'est évoqué nulle part dans le document édité par les chercheurs *d'Alibaba Cloud*.
Selon un des auteurs et directeur principal de la recherche sur l'*AI* de *Alibaba*, *Xian-Sheng Hua*, les gens en chine se souciaient moins de la vie privée, ce qui leurs

[33] HUA, X. *et al., op.cit.,* p.1 [34] HUA, X. *et al., op.cit.,* p.11 [35] HUA, X. *et al., op.cit.,* p.2 [36] HUA, X. *et al., op.cit.,* p.1

permettaient d'aller plus vite [37]. La sociologue *Gemma Clavell* en revanche prononce ses craintes sur la protection des donnés privées dans le système *City Brain* [37]. Sur leur présence internet, *Alibaba cloud* revendique d'être conforme à plusieurs normes de sécurité et protection de donnés comme la *ISO/IEC 27001* et la *EU GDPR* [40].

CONCLUSION

Il est d'intérêt de faire une comparaison entre *City Brain* et *FIWARE* malgré leurs fonctionnements différents car chaque système est reconnu et soutenu par des états d'influences majeures. *FIWARE* profite des fonds de l'union européenne et *City Brain* du soutien de l'état chinois.
Concernant la sécurité des deux systèmes, les divergences ne sont certainement pas immenses car il s'agit dans les deux cas d'une plateforme composée de plusieurs sous-algorithmes qui sont protégés d'accès non-autorisés par des stratégies de sécurisation. Néanmoins une différence majeure repose sur le fait que dans l'exemple open source, la preuve de l'existence de cette instance protectrice est indéniable car elle se manifeste dans le *source code* [41]. *City Brain* en revanche ne fournit aucune preuve fiable d'une existence d'un mécanisme de sécurisation. Il faut faire confiance à ce qui est publié délibérément sur leur site web [42].
La réponse à la question, s'il était plus aisé pour des hackers de développer des virus ayant un accès au source code, serait oui et non. L'information sur la « *DNA* » du logiciel augmente effectivement le risque d'une attaque visée mais une adaptation pour contrer ces failles de sécurité est également plus aisée et rapide [43]. Il faut clarifier de même qu'un accès au code source ne veut pas dire que les clés de sécurités sont exposées à tout le monde. Une clé générée pour une seule instance ne figure dans aucun cas dans le répositoire du projet.
Les systèmes sont tous les deux indéniablement capable de collecter des informations personnelles sur les citadins.
C'est d'autant plus que la question de ce qui se passe avec les données une fois récoltées devient pertinent et constitue une autre différence cruciale entre les deux plateformes. Dans l'exemple *open source*, les données sont sauvegardées et peuvent être lues par une personne autorisée. Une Intelligence artificielle peut être intégrée dans le système [44] pour évaluer des changements anormaux ou des

[37] BEALL, A. *op.cit.* [38] HUA, X. *et al., op.cit.,* p.7 [39] HUA, X. *et al., op.cit.,* p.8 [40] https://www.alibabacloud.com/trust-center?spm=a3c0i.14009044.3156523820.dnavwhyc1.39793f6740eMLg [41] https://github.com/FIWARE/tutorials.Securing-Access ; https://github.com/FIWARE/tutorials.PEP-Proxy [42] https://resource.alibabacloud.com/whitepaper/alibaba-cloud-security-whitepaper---international-edition-v20-2020_1717?spm=a3c0i.8119595.7120358420.1.2277411do8QgrG [43] RING, R. 2012. *Open source, red Hat, and security,* Raleigh, Red Hat Inc. [44] https://github.com/FIWARE/tutorials.Big-Data-Analysis

erreurs. Mais le rôle de ce composant n'est pas de faire des décisions ou de proposer des prédictions contrairement à l'*AI* de *Alibaba Cloud*.
La capacité décisive et la création des bases de données individuelles de *City Brain* constitue une infraction profonde du droit à la vie privée des habitants. La récolte d'informations se passe sans l'accord des individus et est donc inhumaine et devrait être interdite par la loi.
Une autre problématique au niveau de la protection des données est le statut propriétaire une fois récolté et stocké. À qui appartiennent les informations personnelles ? Vu qu'elles ne sont pas protégées par des licences, elles appartiennent à tous ceux qui dispose d'un droit de lecture. La gestion de ses autorisations est donc un élément fondamental pour permettre une protection de la vie privée. Dans l'exemple open source, les droits de lecture sont distribués par l'administrateur, souvent le mainteneur du réseau. Ceci pourrait indiquer un équilibre hiérarchique dans la gestion de la plateforme.
En réalité, l'administrateur n'intervient uniquement comme instance supérieure au moment de la mise en place du réseau, une fois fonctionnel, les droits de lecture seront autogérés et actualisés par les algorithmes. Concernant *City Brain*, ses droits ne sont à aucun moment distribués aux utilisateurs. Il s'agit d'un groupe de personnes sélectionnées pour s'occuper de la gestion de la *smart city* qui ont un accès illimité aux données privées. Ceci est évidemment problématique car il est impossible pour un individu vivant dans une *smart city* gérée par *City Brain*, de savoir si les données seront utilisées uniquement pour optimiser la ville ou si elles seront vendues à des tiers. Il est donc raisonnable de conclure sur l'affirmation que l'emploie d'un système basé ou dérivé de *FIWARE* avec une intégration d'une intelligence artificielle vérifiée, est plus favorable que de baser la gestion de la *smart city* sur des logiciels intelligents avec des codes source inaccessibles comme *City brain*.

BIBLIOGRAPHIE

MONOGRAPHIES:

DETZNER, P. ; SALHOFER, P. 2020. *Proceedings of the 53rd Hawaii International Conference on System Sciences,* Analysing FIWARE's Platform - Potential Improvements, Frauenhofer Institut Dortmund

HUA, X. *et al.* 2019. *The City Brain: Practice of Large-Scale Artificial Intelligence in the Real World,* Hangzhou, IET Research Journals.

ABOSAQ, N. 2019. *Impact of Privacy Issues on Smart City Services in a Model Smart City,* Yanbu, Yanbu University College.

CIRILLO, F. *et al*. 2019. *A Standard-based Open Source IoT Platform: FIWARE*, Heidelberg, NEC Laboratories Europe.

SALHOFER, P. 2018. *Proceedings of the 51st Hawaii International Conference on System Sciences,* Evaluating the FIWARE Platform, FH Joanneum

ELMAGHRABY, A. 2013. *SECURITY AND PRIVACY IN THE SMART CITY,* Ajman, AIUPC.

POTOCZNY-JONES, I. *et al.* 2019. *Encrypted Dataset Collaboration,* Portland, Association for Computing Machinery.

GAIRE, R. *et al.* 2018. *Crowdsensing and privacy in smart city applications*, Canberra, CSIRO.

RING, R. 2012. *Open source, red Hat, and security,* Raleigh, Red Hat Inc.

PÉRIODIQUES:

TEGMARK, M. s.a. « BENEFITS & RISKS OF ARTIFICIAL INTELLIGENCE », *future of life institute*, https://futureoflife.org/background/benefits-risks-of-artificial-intelligence

RADTKE, M. 2019 « Was ist Big Data ? », *Bigdata insider*, https://www.bigdata-insider.de/was-ist-big-data-a-562440

FISCHL, G. 2020. « Mandrake: Android-Schädling stiehlt Daten seit 2016 », *Connect*, https://www.connect.de/news/mandrake-android-malware-stiehlt-daten-apps-play-store-3200783.html

COLLINS, H. 2009. « Is Open Source Software More Secure than Proprietary Products? », *Govtech*, https://www.govtech.com/security/Is-Open-Source-Software-More-Secure.html

BEALL, A. 2018 « In China, Alibaba's data-hungry AI is controlling (and watching) cities », *Wired* , https://www.wired.co.uk/article/alibaba-city-brain-artificial-intelligence-china-kuala-lumpur

SALTIS, M. 2020. « Comparing Open Source Software vs Closed Source Software », *Coredna*, https://www.coredna.com/blogs/comparing-open-closed-source-software

PAGES INTERNET:

Consultable:
https://eu.alibabacloud.com/ [disponible le 19 mai 2020].

Consultable:
https://www.fiware.org/ [disponible le 19 mai 2020].

Consultable:
http://forge.fiware.org/plugins/mediawiki/wiki/fiware/index.php/FIWARE_Privacy_Policy [disponible le 19 mai 2020].

Consultable:
https://www.linux.org/ [disponible le 19 mai 2020].

Consultable:
https://www.fiwoo.eu/blog/ [disponible le 19 mai 2020].

Consultable:
https://github.com/Fiware [disponible le 19 mai 2020].

Consultable:
https://www.alibabacloud.com/trust-centerspm=a3c0i.14009044.3156523820.dnavwhyc1.39793f6740eMLg
[disponible le 19 mai 2020].

Consultable:
https://github.com/FIWARE/tutorials.Securing-Access [disponible le 19 mai 2020].

Consultable:
https://github.com/FIWARE/tutorials.PEP-Proxy [disponible le 19 mai 2020].

Consultable:
https://resource.alibabacloud.com/whitepaper/alibaba-cloud-security-whitepaper---international-edition-v20-2020_1717spm=a3c0i.8119595.7120358420.1.2277411do8QgrG
[disponible le 19 mai 2020].

Consultable:
https://github.com/FIWARE/tutorials.Big-Data-Analysis [disponible le 19 mai 2020].

Consultable:
https://ec.europa.eu/research/fp7/index_en.cfm [disponible le 19 mai 2020].

Consultable:
https://www.redhat.com/de/topics/api/what-are-application-programming-interfaces
[disponible le 19 mai 2020].

Consultable:
https://github.com/telefonicaid/fiware-orion [disponible le 19 mai 2020].

Consultable:
https://fr.wikipedia.org/wiki/%C3%89tat_civil [disponible le 19 mai 2020].

Consultable:
https://www.gnu.org/philosophy/floss-and-foss.de.html [disponible le 19 mai 2020].

Consultable:
https://www.sec.gov/Archives/edgar/data/1124804/000119312508212359/dex104.htm [disponible le 19 mai 2020].

Consultable:
https://www.fiware4water.eu [disponible le 19 mai 2020].

Consultable:
https://synchronicity-iot.eu/ [disponible le 19 mai 2020].

Consultable:
https://autopilot-project.eu [disponible le 19 mai 2020].

Consultable:
https://www.iof2020.eu [disponible le 19 mai 2020].