UNIVERSITÉ DU QUÉBEC À MONTRÉAL

GESTION DE L'IDENTITÉ DES INDIVIDUS SUR PLATEFORMES MOBILES – PROPOSITION DE MODES D'OPÉRATION ET AUTRES EXTENSIONS POST-KNOX

MÉMOIRE

PRÉSENTÉ

COMME EXIGENCE PARTIELLE

DE LA MAÎTRISE EN INFORMATIQUE DE GESTION

PAR

EDUARDO GONZALO AGURTO CATALÁN

JANVIER 2018

REMERCIEMENTS

J'aimerais remercier tous ceux et celles qui m'ont guidé tout au long de ce processus de recherche. L'activité entreprise est ambitieuse et requiert constamment de se faire recentrer afin de préserver le cadre académique dans lequel elle doit se dérouler. J'aimerais donc remercier les correcteurs du présent document qui ont démontré une attention bienveillante et constructive même dans les moments où il fut nécessaire de me forcer à reprendre, réorienter, voire délester le travail. J'aimerais aussi remercier le personnel de soutien du département et de la faculté qui a démontré une grande patience à mon égard. Enfin, j'aimerais remercier l'UQÀM de permettre en ses murs de foisonner de la recherche qui ose tenter d'apporter des changements dans la société. Surtout, j'aimerais remercier mon directeur de recherche, le Pr. Normand Séguin, vice-doyen de l'enseignement de la Faculté des Sciences, pour sa rigueur et sa capacité de suivre un phénomène dont la rapide évolution requiert des cycles de développement serrés.

Enfin, j'aimerais remercier ma famille et mon entourage qui m'ont été d'un grand appui tout au long de cette démarche.

TABLE DES MATIÈRES

LISTE DES FIGURES

LISTE DES TABLEAUX

LISTE DES ABRÉVIATIONS, SIGLES ET ACRONYMES

API	De l'anglais, « *Application Programming Interface* », interface programmatique
BYOD	De l'anglais, « *Bring Your Own Device* ». Politique d'entreprise sur l'informatique mobile permettant aux employés d'utiliser, dans le cadre de leur travail, leurs propres appareils électroniques.
CST	Centre de la sécurité des télécommunications
DRM	De l'anglais « *Digital Rights Management* », gestionnaire des droits numériques; systèmes logiciel de protection permettant de s'assurer que seuls les ayant droits légitimes ont accès à du contenu protégé par de la propriété intellectuelle
GAFA(M)	Google, Apple, Facebook et Amazon, les géants du web. Microsoft figure parfois dans cette liste, mais usuellement s'en trouve exclue.
GIDI	Gestion de l'identité des individus
GIDI(M)	Gestion de l'identité des individus s'étendant aussi sur plateforme mobile
GIDIM	Gestion de l'identité des individus sur plateforme mobile
GL	Génie Logiciel
LCCJTI	Loi concernant le cadre juridique des technologies de l'information, L.R.Q. chapitre C-1.1 (http://www.legisquebec.gouv.qc.ca/fr/showdoc/cs/C-1.1).
MADA	De l'anglais, « Mobile Application Distribution Agreement », contrat conditionnant la distribution d'applis sur Google Play.
MDM	De l'anglais, « *Mobile Device Manager* », gestionnaire d'appareils mobiles; solution logicielle et parfois matérielle servant à gérer un parc d'appareils d'informatique mobile
NSA	De l'anglais, « *National Security Agency* », pendant américain du CST du Canada.
OAS	Opérateur d'applications et de services

OP	Opérateur de plateforme
OT	Opérateur de télécommunications
PDA	De l'anglais « *Personal Digital Assitant* », dispositif électronique personnel et portable antécédent aux téléphones intelligents
SOX	Loi Sarbannes-Oxley
TCG	De l'anglais, « *Trusted Computing Group* », anciennement « *Trusted Computing Platform Alliance* », organisme œuvrant à la promotion de l'informatique de confiance
TIC	Technologies de l'information et des communications
UF	Utilisateur final

RÉSUMÉ

L'élicitation des besoins des utilisateurs est normalement le fondement initial derrière le développement du logiciel, la littérature du génie logiciel en ce sens est bien établie. Or, pour les logiciels grand public (« *shelf software* »), c'est rarement le cas. Dans un contexte où l'informatique devient à la fois très personnelle et fondamentale au fonctionnement des sociétés, cette inadéquation soulève plusieurs problématiques allant de l'individu (ex : vie privée) jusqu'aux nations (ex : souveraineté technologique). Le cas de la Gestion de l'Identité des Individus sur plateformes Mobiles (GIDIM) est un cas où le développement suit plutôt les exigences émanant principalement de divers opérateurs selon diverses considérations de pouvoir et de rentabilité. Or, s'est constitué une niche de marché pour répondre à cette inadéquation auprès certains profils de clients, principalement les employés utilisant Knox sur des téléphones Samsung. Cette distinction est extensible de manière à intégrer davantage les besoins des utilisateurs, lesquels ne peuvent être recensés directement. Une approche indirecte, par la revue de la littérature et des rapports de consultations publiques et d'autres sources, a permis de déceler, malgré le vaste nombre et la grande diversité des utilisateurs et de leurs besoins, des modes d'opération correspondant à des contextes d'utilisation. Ces besoins peuvent être validés par le fait qu'il existe des applications qui essaient, tant bien que mal, de répondre à ces besoins qui seraient probablement mieux servis au niveau système. La présente étude propose des modes identifiés et à décrit sommairement les principaux rapports et interactions que ceux-ci peuvent avoir entre eux afin de paver la voie à des études et efforts subséquents visant à mieux comprendre et intégrer les besoins des utilisateurs dans la GIDIM.

Mots clés : GIDIM, identité, vie privée, exigences des utilisateurs, droits numériques, etc.

ABSTRACT

Under the prescriptions brought forth by the best practices and recommended methodologies of Software Engineering, the software development process shall start by the elicitation of the requirements from the users. This should be of particular importance in the field of personal computing, with a strong emphasis on technologies that are key to the user experience of the modern digital life, namely mobile devices. However, despite the great importance that user requirements shall bear in this context, the development of mobile device platforms as well as of applications is driven mainly by the platform operators and in absentia of any explicit mechanism to capture the user's needs, requirements, preferences and so on. This is a striking paradox when it comes to Identity Management (IDM), more precisely, Mobile Identity Management (MIDM). Some improvements have been brought to light from the monolithic default options offered by native platforms and mods. The most significant advances towards expressing the user's needs in terms of MIDM is Knox, by Samsung. Despite these efforts, the main focus of Knox is yet rather oriented towards the needs of the user's employers, not the users themselves. To this state of fact, this paper presents research performed on a documentary data set in order to elaborate a model of user needs. Then, from the requirements identified, it derives certain extensions to the current default MIDM mechanisms offered by Apple's iOS and Google's Android platforms. Furthermore, it proposes a set of modes of operations (sorts of use cases) or scenarios as well as a model to organize them and integrate them.

Keywords : BYOD, Mobile Identity Management, user requirements, digital rights, social software engineering

CHAPITRE I

INTRODUCTION

Le développement des technologies de l'information et des communications (« TIC ») accroît grandement les capacités applicatives (la *facultatem ad faber*) des utilisateurs, d'une manière inouïe et croissante. Cela rend l'adoption de diverses technologies, dont l'informatique mobile, très répandue. Or, cette adoption propose bien entendu, d'une part, les nouvelles possibilités qui s'y rattachent, mais d'autre part, parfois de prendre position par rapport à des considérations fondamentales. Ces considérations fondamentales sont nombreuses et s'articulent autour des implications en matière de pouvoir que l'on concède à divers opérateurs sur nos données. Elles sollicitent l'attention du public pour définir la société dans laquelle nous désirons vivre. Or, les utilisateurs sont peu familiers avec ces considérations, malgré le fait qu'elles aient des effets majeurs dans la durée. Par conséquent, elles n'ont pas, ou très peu, fait l'objet, au Québec, d'une mobilisation organisée ou d'un débat public concluant, ce qui serait nécessaire à l'élaboration d'une position commune définie, du moins localement. Bref, les téléphones mobiles intelligents sont populaires [1], mais personne ne semble avoir pris le temps de se demander si leur fonctionnement pourrait mieux répondre à nos besoins et à nos valeurs. Les masses prennent ce qu'il y a en l'état et laissent le soin à d'autres de décider des tenants et aboutissants techniques et opérationnels.

Par moments, des sursauts réactifs traversent l'opinion publique, comme ce fut le cas encore dernièrement avec les révélations [2] au sujet de la surveillance policière des journalistes, dont MM. Patrick Lagacé [3] et Michaël Nguyen [4], dont les causes judiciaires sont encore en attente. L'importance d'avoir des communications sécurisées ainsi que, plus largement, une GIDIM appropriée, sont réapparues comme des fondements d'une saine démocratie [5] à l'ère numérique. Divers débats sous-jacents sont apparus comme importants et mûrs, du moins assez pour que le gouvernement du Québec trouve que la situation méritait de déclencher le processus prévu à cette fin lorsqu'il y a une problématique d'importance, soit de mettre sur pied une commission d'enquête sur la question. En l'espèce, c'est la Commission Chamberland

(officiellement nommée « Commission d'enquête sur la protection de la confidentialité des sources journalistiques » [5]), du nom de l'Honorable juge Jacques Chamberland de la Cour d'Appel, emprunté au plus haut tribunal du Québec, pour la présider. Ainsi, le sujet est brûlant d'actualité et les audiences et débats de cette commission se tiennent au moment même de mettre sous presse, le tout est enregistré et sténographié, en plus des mémoires qui y sont soumis, voilà une mine d'informations au sujet des divers intérêts des principales parties prenantes de la population. Par ailleurs, ce n'est ni le premier endroit, ni la première juridiction où il y a des remous sur cette question et où ces préoccupations sont apparues et ce n'est pas la première fois dont ces convulsions ponctuelles éveillent des populations. Déjà en 2013, Edward Snowden révélait [6] , par le partage avec le « *International Consortium of Investigative Journalists* » (Consortium International pour le Journalisme d'Enquête), ce que plusieurs soupçonnaient déjà [7] : l'espionnage massif des citoyens américains et étrangers, dont alliés, au travers de divers techniques et grâce aux moyens avancés d'agences gouvernementales et à la collaboration des principaux opérateurs de plateforme, ci-après « OPs ». Dans un cas comme dans l'autre, les appareils mobiles jouent un rôle primordial en tant que point de capture de données de notre vie numérique et les mêmes grands acteurs, essentiellement Google et *Apple*, se retrouvent fortement impliqués à tous niveaux.

Or, malgré l'importance du sujet, il n'y a que très peu de réflexion et de recherche sur le sujet des causes techniques (architecturales, relatives à la conception des systèmes ou à leur opération, etc.) de ce phénomène, de ce qui rend cela matériellement possible à la base. Ce vide est autant plus prononcé dans la littérature scientifique et ce n'est pas fortuit. Le sujet est difficile à adapter aux contraintes de la méthode scientifique et son interdisciplinarité pose des difficultés méthodologiques supplémentaires. Un angle d'attaque pertinent peut être celui de la gestion de l'identité (ou des identités, sur systèmes informatiques) mobile(s), la GIDIM. Cependant, au brut, ce sujet est tellement vaste qu'il faut s'y retenter à quelques reprises pour réussir à le focaliser avec suffisamment de précision pour pouvoir y circonscrire correctement un objet d'étude dans un cadre académique, même exploratoire, comme visent les contraintes imposées au présent mémoire. Il n'est cependant pas de la prétention du présent exercice de tenter d'apporter une réponse définitive à l'intégralité d'un sujet aussi complexe et humain. L'humble prétention du présent exercice de recherche est donc d'identifier un aspect important de cette problématique, de l'aborder sous un angle pour lequel

il existe de la littérature académique et d'autres sources, de recenser l'état de la connaissance jusqu'au moment présent, de proposer un modèle exprimant les besoins, de proposer une amélioration aux derniers développement de la situation actuelle (Knox) et de proposer des pistes de réflexion; tels sont les objectifs du présent exercice, de la présente activité de recherche.

D'abord, la bonne nouvelle est qu'il y a des disciplines établies qui soient assez proches du phénomène observé pour pouvoir y puiser plusieurs emprunts. L'approche abordée est celle du génie logiciel (ci-après « GL ») appliqué à l'informatique de gestion. En l'espèce, il s'agit d'un ensemble de principes et de procédés qui permettent de développer des logiciels de meilleure qualité afin de répondre à un besoin de gestion. Plus spécifiquement, le présent exercice va se pencher sur l'étape de l'étude des besoins, une étape essentielle à la fois en génie logiciel et en informatique de gestion.

D'abord, il est de mise de préciser que cette étude n'en est pas une portant sur le génie logiciel, ni réclamant en faire partie. Tout au plus, elle s'en inspire des processus d'analyse portant sur l'élicitation des besoins de manière itérative et incrémentale, des moyens de conciliation de besoins divergents et de quelques formalités dans l'expression des exigences qui en résultent. Le présent travail demeure donc un exercice d'informatique de gestion.

Maintenant, le plan général de recherche étant brossé et la vicinité phénoménologique étant déterminée et délimitée, il serait pertinent, avant de commencer, d'esquisser le chemin ou le sillon que l'on désire tracer par la présente étude dans une tentative d'étendre le territoire connu et recensé académiquement. Cela requiert notamment de comparer en quoi la présente étude compte se différencier des travaux antécédents qui, soit ne couvrent pas le sujet ou ne sont pas menés sous une méthodologie académique. Puis, il faut cadrer l'étude dans sa dimension historique. Ensuite, il serait de mise de clarifier le rôle que le génie logiciel viendrait jouer, à l'intérieur de la portée limitée plus haut, dans cette recherche en informatique de gestion. Cette clarification a plusieurs motifs, dont celui d'éviter d'avoir de conflits méthodologiques entre ces deux disciplines. Le GL a pour but d'assurer une rigueur dans les processus de développement du logiciel, il dispose d'outils particulièrement utiles à la conciliation et à l'intégration de besoins

humains, même lorsque ceux-ci sont incohérents, épars ou ambigus. Enfin, la dernière sous-section abordera succinctement certaines considérations « méta », dont les contraintes propres au contexte académique applicable, les travaux antécédents et l'évolution de ceux-ci jusqu'à la présente mouture.

1.2 Présentation différentielle de la démarche

D'abord, la principale différence entre les préceptes généralement reconnus dans le *SWEBOK* et ceux qui guideront la présente étude se rapportent à l'activité de gestion, laquelle sera atypique par rapport au « *testbed* » en trois parties de Rzepka [6] ou au processus incrémental de Southwell [15]. Cette nuance est nécessaire puisqu'il s'agit d'un processus *in absentia*, mais qui reprend plusieurs préceptes et sous-processus communs dans l'élaboration des modèles sur la base des besoins des utilisateurs, au cours d'itérations successives.

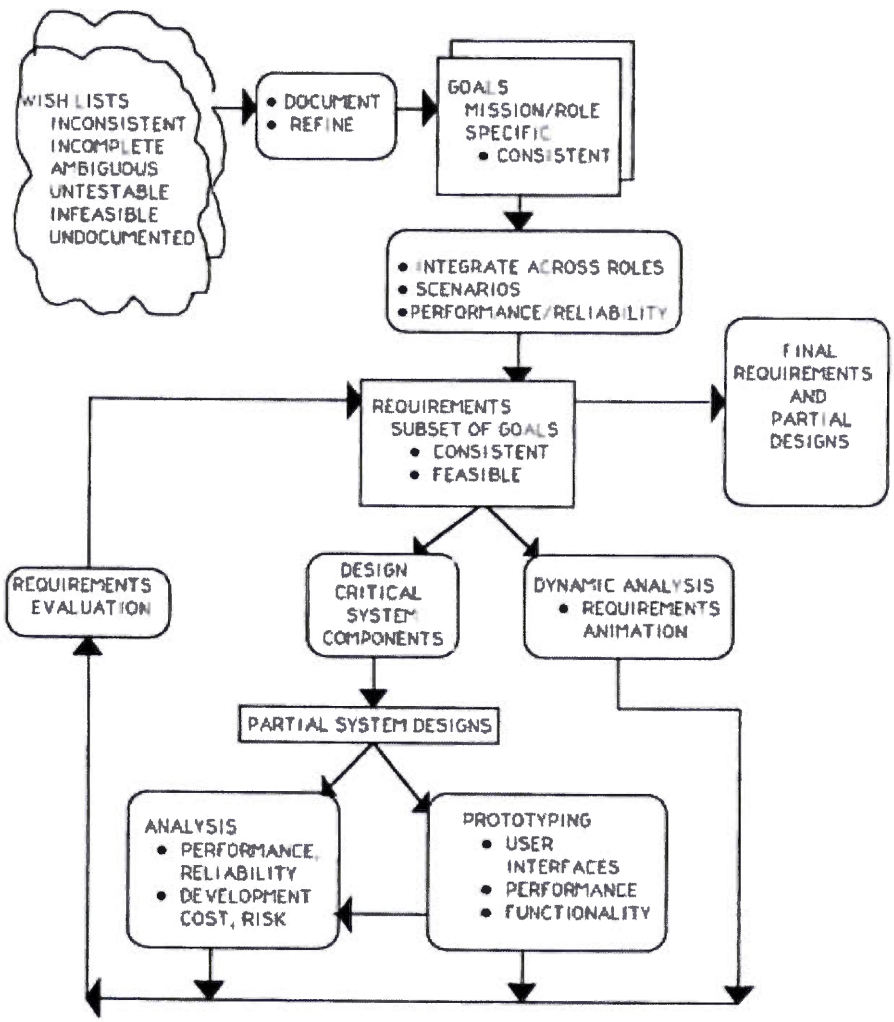


Figure 1.1 – Modélisation du processus de l'ingénierie des exigences
Source : A REQUIREMENTS ENGINEERING TESTBED: CONCEPT AND STATUS, William E. 5Rzepka , 1989

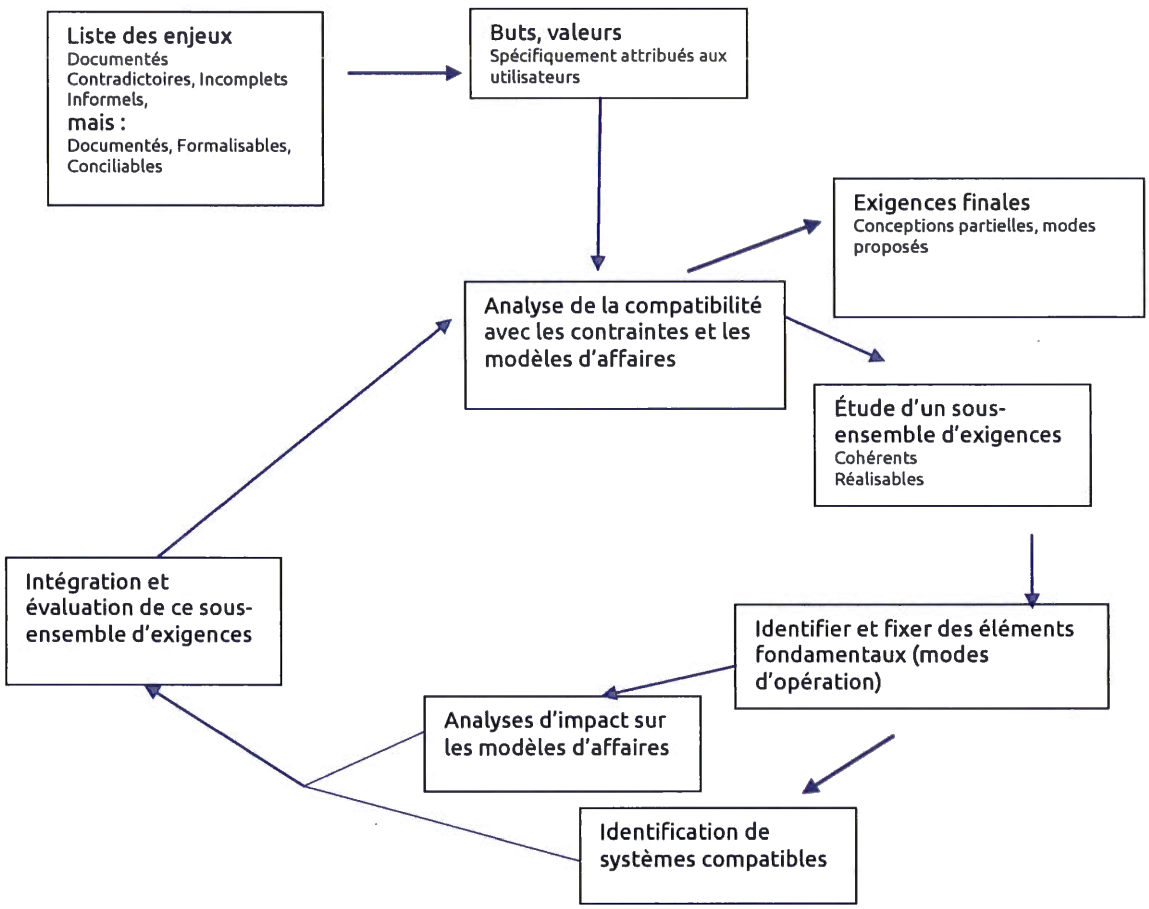


Figure 1.2 – Modèle itératif adapté d'éliciation des besoins des utilisateurs, *in absentia*, en matière de modes d'opération eu regard des modèles d'affaires
Adaptée de : *A REQUIREMENTS ENGINEERING TESTBED: CONCEPT AND STATUS*, William E.Rzepka , 1989

Normalement, c'est un commanditaire qui est à l'initiative du processus d'élicitation des besoins et ce processus est opéré incrémentalement par itérations (successives) auprès d'une population restreinte et organisée d'utilisateurs et de parties prenantes. Que faire lorsque que les besoins que l'on désire éliciter sont ceux d'une population qui constitue une société entière dispersée sur l'ensemble d'un territoire comme celui du Québec? Aucune réponse préexistante n'a été identifiée dans la littérature puisqu'il s'agit de technologies sociales, de technologies dont le déploiement et l'adoption constituent un (nouveau) phénomène social et

dont l'évolution n'est pas la même que pour le développement de technologies commandées par un commanditaire, souvent du fait qu'il n'y pas d'autorité centrale ou publique derrière ce déploiement, mais un ensemble d'individus qui adoptent [8] (ou non) une technologie, au fur et à mesure de son développement, ce qui s'avère une situation beaucoup plus complexe. De plus, il n'y a pas de processus formel bidirectionnel qui guide le développement en regard de l'expression des souhaits des utilisateurs, et même lorsqu'il y a de tels processus, l'implication de la part des utilisateurs est très limitée [9]. Or, la nature de la technologie ou de son adoption ne rend pas moins pertinentes les considérations de génie logiciel. Il demeure légitime de se poser des questions au sujet de l'amélioration structurée et méthodique possible de ces technologies et il faut d'abord définir et circonscrire ce que l'on désire améliorer.

Une fois le plan établi, il est de mise de justifier la portée et les moyens au regard de l'importance du sujet. L'importance du sujet, hormis les considérations fondamentales et théoriques, se justifie par le fait qu'une partie de plus en plus grande de notre quotidien devient de plus en plus dépendante des TIC, et des technologies mobiles en particulier et on atteint un seuil marquant : avec l'avènement des technologies financières (« *fintech* ») [10 et 11] et civiles (« *civtech* ») [12, 13 et 14], ainsi que l'informatisation des guichets de service gouvernemental. C'est la capacité de subvenir à ses besoins et d'interagir avec l'État, voire d'y solliciter son secours et de participer à la vie démocratique, qui basculent dans cet univers où l'identité est un élément fondamental de ces interactions, mais où sa gestion et plusieurs de ses politiques sont conçues par d'autres et selon les besoins d'autrui. De plus, le discours néolibéral promeut la responsabilité sociale individuelle [16]; bref, si les utilisateurs finaux (ci-après, souvent « UFs ») désirent que cela change, ils doivent s'impliquer. Tout d'abord, il leur faudra prendre conscience que les choix qu'ils (également citoyens) effectueront, parmi leurs options limitées, qu'ils exerceront en adoptant une technologie ou un autre, auront des conséquences importantes, principalement au niveau social et cela requiert une perspective à long-terme et interdisciplinaire afin de comprendre tous les tenants et aboutissants, toutes les conséquences de décisions qui peuvent sembler souvent techniques et anodines. Cela requiert un effort intellectuel important et peu nombreux semblent être ceux et celles qui sont prêt(e)s à investir cet effort. L'équilibre entre les intérêts et exigences des différentes parties prenantes se reflète dans la conception du logiciel, du matériel et de l'infrastructure qui sont nécessaires à l'exploitation et l'utilisation de technologies mobiles et cela a des effets durables, sur plusieurs générations. La question des effets dans la durée des décisions de génie logiciel

sur les sociétés a déjà été abordée, notamment dans le chapitre « *The Impact of Software on People and Society* » de la monographie « *Technical and Social History of Software Engineering* » (2014) [18] de Caper Jones et et « *Designing for Social Impact* » (s.a.) [19] de Gretchen Anderson. L'intersection même entre le génie logiciel et les enjeux sociaux s'appelle le génie logiciel social (« *Social Software Engineering* ») et a même connu des rencontres spécialisées en 2011 et 2016. Ce domaine a été documenté [20] par Ahmadi et al., en 2008.

Au moment présent, ces décisions sont principalement prises pour les UFs par les opérateurs de plateformes, lesquels n'ont pas nécessairement les mêmes intérêts que ces UFs, comme il sera exposé ultérieurement dans la présente étude. Il demeure donc légitime et même d'un grand intérêt académique de se prêter à combler ce vide et à étudier de manière méthodique, idéalement dans une démarche neutre et désintéressée, les besoins des utilisateurs, ou du moins ceux que le chercheur assumera de leur imputer.

Précisément, c'est là que se rencontre la deuxième limite particulière à cet objectif de recherche. Dans l'absolu, il faudrait demander à chaque individu concerné quels sont ses besoins et trouver un modèle d'intégration afin de faire entrer en adéquation les données obtenues des besoins recensés et le modèle de besoins proposé. Souvent, les données peuvent pointer vers des besoins divergents, voire inconciliables, ainsi que sur des niveaux de réflexion incomparables face à cette élicitation.

Il existe normalement diverses techniques de conciliation comme celles proposées [21 et 22] par JA García-García, M.J. Escalona et E Ravel (2012, 2014) ou bien Mark Blackburn, Robert Busser et Aaron Nauman [23 et 24] (du « *Software Productivity Consortium* », 2004), mais celles-ci sont difficilement adaptables à une population aussi générale. Même un échantillon tiré aléatoirement ou stratifié [25] de manière à recomposer une sorte de miniature de la population totale pose des problèmes théoriques, de par le nombre de dimensions d'analyse pertinentes pour lesquelles la variance doit être contrôlée et conforme aux intervalles de confiance que l'on désire adopter, et tout cela sans même parler de la praticabilité matérielle de la chose et des ressources nécessaires à cet effet. En plus, on ne connaît pas, à la base, les dimensions pertinentes puisqu'il n'y a pas d'études antécédentes auxquelles se comparer.

Même faisant abstraction de ces contraintes méthodologiques, il faudrait du moins trouver un échantillon représentatif de la population et le sonder sur ces questions. D'ailleurs, à titre exploratoire, cela fut fait antérieurement et les conclusions peuvent se résumer ainsi : les besoins sont très divers et inconciliables, ils se regroupent essentiellement par grappes et des profils d'utilisateurs; enfin, ils sont fortement tributaires du contexte, pour un même utilisateur, ils peuvent varier grandement en fonction du rôle que l'utilisateur exerce sur son téléphone : parent, amoureux, employé, coach, amant, etc.

Pour ces motifs, la présente démarche ne vise pas à dégager intégralement un modèle des besoins ou un modèle des exigences, mais seulement une partie de ceux-ci, celle visant à exprimer un ensemble de modes d'opération (ou « modes opératoires ») et leurs mécanismes de GIDIM correspondants. L'élaboration de ces modes vise à englober la plupart des besoins identifiés dans des itérations antécédentes et qui sachent également être compatibles avec les modèles d'affaires, les motifs de cette deuxième contrainte étant explicités ultérieurement. Les modes opératoires sont des ensembles de paramètres et configurations visant à établir un contexte d'utilisation précis. Par exemple, le « mode avion » permet d'utiliser le téléphone sans émission RF. Le mode silencieux permet son utilisation sans émettre de son. En généralisant l'idée, voici donc des modes ultra simples, mais ceux-ci peuvent être infiniment plus complexes et subtils afin de répondre à des contraintes opérationnelles plus sophistiquées.

Ensuite, même en connaissant les besoins des utilisateurs, il faudrait un vecteur permettant d'intégrer ces besoins au cycle de développement, ce qui requiert un agent pour ce groupe hétérogène et qui pose un problème intrinsèque de légitimité et de représentativité. L'agent résiduel de la population est l'État. Or, les pays (États-Unis, Royaume-Uni, Japon, Corée, Chine) où se sont essentiellement développées, au cours des dernières décennies, les technologies de l'information en général, ainsi que les technologies mobiles en particulier, présentent une philosophie néolibérale et une tendance au désengagement de l'État en matière d'impératifs opérationnels aux entreprises privées, ce qui rend assez lointaines les dernières expériences de développement de technologies sociales organisées selon des préceptes où les utilisateurs ont leur mot à dire; bref, de consultation publique au sens large. Pour mémoire, le développement du Minitel (le service plus que la technologie), en France, a fait l'objet d'une certaine participation citoyenne. Autre temps, autres mœurs.

Or, depuis quelques années, la participation citoyenne dans les débats politiques a regagné du terrain, notamment au travers des technologies de l'information et de la communication, lesquelles permettent de relever des défis que peuvent parfois poser la distance ou la logistique nécessaires à réaliser de telles consultations. Les efforts distribués autour des préceptes de développement libre ont le vent dans les voiles [26] et, au Québec, la prise de parole des citoyens est vivement encouragée. Ainsi, de nos jours, la voie privilégiée pour connaître les intérêts et les besoins de la population est la consultation publique accessible en personne ou en ligne, ce format permettant d'éliciter tous les besoins particuliers de chaque groupe ou individu pour qui ce besoin est suffisamment important pour le motiver à venir s'exprimer devant la Commission qui préside la consultation ou déposer un mémoire auprès de celle-ci. Un des avantages de cette démarche est qu'elle permet de produire des actifs documentaires et d'en connaître les auteurs. Cela a notamment été le cas pour la Commission Bouchard-Taylor [27] sur les pratiques d'accommodement (2006-2008), mais également pour la Commission Charbonneau [28] (enquêtant) sur l'octroi et la gestion des contrats publics dans l'industrie de la construction. Une telle approche a comme avantage principal sur les sondages (dont ceux aléatoires) qu'il permet à tout besoin suffisamment pressant (impulsé sous une pression suffisante pour en motiver l'expression), d'être exprimé. Cela permet d'avoir une approche exhaustive des besoins, sous l'hypothèse que tout ce qui avait à être exprimé l'a été. Donc, les populations sont capables d'exprimer leurs besoins de manière structurée, il existe déjà des processus bien rodés à cette fin.

Néanmoins, il demeure rare que le développement de technologies utilisées par les masses soit sujet à de telles consultations puisque le développement de technologies est surtout une affaire privée et le modèle d'évolution des exigences correspond, d'ordinaire au développement logiciel mené par le marché, tel que décrit [29, 30, 31 et 32] par L. Lehtola et M. Kauppinen. Il y a cependant un changement de mœurs qui s'inscrit dans la tendance de regain de la démocratie au travers des TIC décrit plus haut et il s'agit des la diversité des consultations publiques qui ont lieu en ce moment. C'est dans cette perspective, et dans le cadre d'une étude documentaire que ces Commissions, leurs heures de médias et leurs milliers de pages de documents et transcriptions, sont une réelle mine d'information pour les chercheurs. Similairement, l'Union Européenne et les pays scandinaves membres ou non de l'Union Européenne, sont les plus avancés en la matière sur cette voie, en ce moment.

Notamment, la Suède a tenu de telles consultations en prévision de la virtualisation intégrale de la couronne (monnaie) suédoise. Une autre initiative en ce sens, de la plus récente actualité (dont les travaux se sont déroulés du 18 avril au 7 juin 2017), est celle sous l'égide de l'organisme *REISearch*, endossé par la Commission Européenne, cherchant à joindre dix (10) millions d'individus et s'organisant autour de la série d'initiatives du thème « *Next Generation Internet* », (Internet prochaine génération). Ces consultations visent à recenser les besoins, inquiétudes et perceptions des citoyens en lien avec l'évolution de l'Internet. Les consultations thématiques sur la neutralité de l'internet, l'intelligence artificielle, la vie privée et les technologies financières sont celles qui ont sollicité le plus d'expression de la part du public. *REISearch*, contrairement aux autres initiatives de consultation publique, vise la capture de résultats qui furent présentés à l'occasion d'un congrès, point culminant de l'évènement. Les conclusions essentielles de la présentation du rapport [33] (2017) de ce congrès sont à l'effet que les populations recensées présentent des inquiétudes récurrentes face à l'évolution de l'Internet et réclament plus d'autodétermination.

Avec recul, notons que la méthodologie des commissions et consultations publiques n'est cependant pas très discriminative, elle ne vise pas le développement de connaissances de niveau académique et prend en intrant tous les documents qui sont déposés, qu'ils aient été produits dans un contexte commercial, individuel, académique, militant, associatif ou autre. Il n'en demeure pas moins que voilà un point de référence qui pourrait être un excellent pivot de départ pour une activité de recherche telle celle documentée par la présente étude. Cependant, trois observations doivent être respectées : d'une part, il faudrait y apporter des adaptations et des resserrements méthodologiques pour que cela puise cadrer avec les exigences d'une activité de recherche académique, et, d'autre part, il faudrait aussi focaliser la portée et d'en étendre la démarche puisque le résultat recherché comporte une proportion d'amélioration de la situation actuelle, ce qui requiert d'intégrer également des éléments purement techniques à la présente étude et d'aller au-delà du seul modèle des besoins pour aboutir vers un sujet très précis : la GIDIM. Au surplus, la différenciation entre la méthode retenue par *REISearch* ou la Commission Chamberland et celle qui sera retenue dans la présente étude est confirmatoire et a *posteriori* puisque la présente étude a démarré il y a plusieurs années et, même sous sa dernière mouture, demeure plus ancienne que les (antécédente aux) travaux de *REISearch*. Ainsi, les méthodes retenues par ces initiatives

viennent confirmer la validité de certains éléments de la démarche de la présente étude, soit : l'importance accordée à la législation et à la jurisprudence dans l'étude des besoins et des contraintes, l'admission de la littérature technique et associative ainsi que, plus fondamentalement, la pertinence de la démarche d'élicitation des besoins des utilisateurs.

Par ailleurs, il faut rappeler que la réflexion relative aux « besoins des utilisateurs » en matière de GIDIM a également été abordée dans le contexte de l'entreprise. Ainsi, depuis nombre d'années déjà, il existe des solutions de types gestionnaire d'appareils mobiles (« *Mobile Device Management* », ou « MDM »), lesquels intègrent et ont déjà produit ou induit un corpus important de littérature technique [34, 35, 36, 37, 38, 39, 40, 41, 42, 43, ...] (et parfois scientifique [44, 45, 46 et 47]), notamment en matière de GIDIM. Or, ces approches sont essentiellement des approches de besoins « pour les utilisateurs », généralement menées et sujettes à l'expression, avant tout, des priorités des employeurs ou des institutions (scolaires, paramilitaires, académiques, associatives, etc.) qui désirent faire valoir leurs droits et qui constatent, elles aussi que ceux-ci ne sont pas nécessairement alignés avec les prérogatives des opérateurs de plateforme telles qu'elles s'expriment dans les paramètres par défaut.

Enfin, une fois la présente activité de recherche esquissée, il est important de l'inscrire dans son contexte historique puisqu'elle vise une évolution possible, donc une transition d'état, et sans connaître les étapes antérieures de l'évolution qui ont mené à la situation actuelle, il y a un risque réel de pointer vers des états que l'on sait déjà aboutir vers des situations problématiques. Par exemple, si on fait abstraction des motivations historiques qui conditionnent le niveau de prise en charge plus élevé que l'on rencontre chez *Apple*, on pourrait commettre l'erreur de proposer des solutions qui ne prendraient pas en compte la réalité d'affaires (ex : l'importance de *iTunes* et du contrôle *DRM*) et qui demeureraient impraticables. Similairement, on pourrait aussi proposer des solutions qui ont déjà été visitées sans obtenir des résultats concluants; de là la pertinence de la prochaine sous-section.

1.3 Historique

A priori, il faut comprendre que la GIDIM est un domaine de recherche très récent et qu'il s'inscrit dans le cadre plus large de la GIDI, ainsi que, de l'informatique de gestion orientée sécurité. Il faut également garder à l'esprit que, depuis ses débuts de la Pascaline [48], l'informatique vise à surmonter, par l'automatisation que celle-ci procure, soit qu'elle prenne forme par les premières formes de mécanisation [49] ou bien qu'elle relève de l'intelligence artificielle quantique [50], divers défis présentant des caractéristiques particulières rendant cette automatisation avantageuse face à ce genre de problèmes. Parmi les plus importantes grappes de défis ayant contribué historiquement au développement de l'informatique, il y a les questions militaires (balistique, cryptanalyse), les calculs scientifiques ainsi que les difficultés propres à la gestion des volumes d'information qui surviennent lorsqu'il y a des relations hiérarchiques entre une institution centrale qui cherche à exercer une autorité sur une population et les *n* membres qui constituent cette population. Sous ce créneau, on peut considérer que l'informatique traîne, de par son historique ainsi que par la concentration des ressources qu'elle a longtemps nécessité, un passif et un penchant favorable à une objectivisation de l'individu. Bref, elle est la systématisation quintessentielle de l'idée du « dossier # » servant à exprimer abstraitement une individu, nonobstant toute son humanité et sa complexité. Ce n'est que très récemment, au cours des années 1970, qu'il y a eu des mouvances qui se sont organisées autour de la défense des droits des utilisateurs et l'idée du « #jenesuispasun# ».

Ensuite, en avançant de quelques décennies, jusqu'à la fin des années 1990 ou le début des années 2000, à l'origine des appareils mobiles, qu'il s'agisse de PDAs, des Blackberry ou du premier *iPhone*, la situation était assez verrouillée, tout comme l'était celle des appareils de bureau dans les premiers temps ou seuls IBM OS/2 et Mac OS (classique) étaient, pour le grand public, les principales options disponibles à survivre. L'ouverture d'éléments fondamentaux tels le système d'exploitation est venue très rapidement dans le cas des appareils mobiles, même avec la série N800 de Nokia sous Maemo, puis avec *Android*. L'Histoire retiendra que la plateforme à code source ouvert *Android* fut rapidement introduite pour rivaliser [50, 51 et 52] avec *iOS* d'*Apple*. Le choix d'adopter une technologie ouverte fut tributaire des conditions particulières de ce contexte : Google cherchait à rattraper son retard

et les principaux déficits qu'il connaissait face à *Apple* à ce moment étaient de taille : Google ne produisait pas d'appareils mobiles et il y avait une panoplie d'applications déjà développées pour le *iPhone*. Du côté des avantages, Google détenait déjà son service Google Maps, duquel dépendait le *iPhone*, jusqu'à sa version *iOS* 4, et pour lequel les utilisateurs de l'*iPhone* représentaient une portion importante des utilisateurs; les deux géants se tenaient donc par la barbichette. Lorsque Google décida d'acheter *Android* [53, 54 et 55], en 2005, l'approche retenue à la base en était une centrée autour d'un noyau Linux [56, 57, 58, 59 et 60], avec tout ce que cela implique philosophiquement. Notons que Google a une approche amicale envers le développement en code source ouvert [61, 62, 63, 64 et 65], du moins pour les éléments de logiciels qu'elle déploie chez les masses, tout en restant souvent assez discrète relativement aux technologies [66, 67 et 68] qu'elle utilise pour ses propres infrastructures ou bien au cœur des appareils (« *appliances* ») [69] qu'elle louait ou vendait sous une formule gardant ses clients très rapprochés de son influence, souvent leur publication suit leur usage interne.

Néanmoins, en matière de stratégie commerciale, selon l'analyse de ses rapports financiers [70 et 71] (2011), Google (maintenant « *Alphabet* ») semble avoir vite compris que la valeur ajoutée se trouve dans l'exploitation de services et non dans le développement de logiciels ou la manufacture de matériel. Ces deux activités ne servent qu'à titre d'activités de support, de manière à améliorer la qualité ou à réduire les coûts. Lorsque ni l'une ni l'autre de ces motivations ne semble être favorisée, ce genre d'activité n'est généralement pas poursuivie, du moins pas à l'interne. Elle est alors externalisée. Par exemple, Google ne produit pas (ou presque pas) de téléphones (excepté épisodiquement des Nexus et Pixel, et précédemment quelques rares, Motorola). Tout au plus, lorsque Google acheta Motorola (division *Mobility*, mais *Home* aussi), il appert que ce sont principalement les brevets qui étaient visés et la compagnie (ou sa division *Motorola Mobility*) fut revendue à *Lenovo* [77] en ce qui a trait aux opérations. Tout comme Google, *Apple* a aussi externalisé certaines activités. Le coup de génie de Steve Jobs à la sortie du *iPhone* fut de rendre le produit suffisamment désirable pour convaincre les compagnies de téléphonie/télécommunications mobile de financer indirectement le développement du *iPhone*, c'est-à-dire d'en externaliser le financement [73, 74 et 75]. Cela fut un pari réussi, mais très risqué, qui se fit en trois mouvements. *Apple* présenta d'abord son prototype, puis mit les opérateurs télécommunications (« OTs »), pays par pays, en concurrence pour obtenir l'exclusivité de vente de son produit

révolutionnaire [75]. La contrepartie de cette exclusivité portait des conditions nombreuses et confidentielles, qui demeurent encore secrètes, mais au sujet desquelles il y a eu quelques fuites dans les canaux non-officiels. Parmi ces conditions, on y trouve notamment celle, pour l'opérateur de télécommunications, de vendre l'appareil à un prix inférieur au coût d'achat que celui-ci paiera auprès d'*Apple* [76, 78 et 79]. En faisant cela, *Apple* transfère son risque relatif à la vente des appareils aux OTs. Ce sont aussi eux qui devront financer la différence des prix (marge négative), ce qui augmente leur risque de ne pas être payés. Tout cela a conduit les opérateurs (de plateforme et de télécommunications) à tenter de maximiser le contrôle autour du client, de manière à mitiger ces risques. *Apple* avait donc un incitatif d'aller dans ce sens. Parmi les exemples de tels contrôles : la conception initialement compatible avec un seul type de signal (au Canada : GSM, celui opéré par le partenaire opérateur de télécommunications national, Rogers et al.), le verrouillage des téléphones (« *locking* ») afin qu'ils ne puissent être utilisés sur un autre réseau (même s'il est compatible) ou dans un autre pays. Ce verrouillage ne peut souvent être enlevé que de manière complexe et uniquement si le client est en bons termes avec son OT (il a payé ses comptes à jour, il a honoré la durée prescrite du contrat, etc.) et souvent accompagné de la restriction de certaines fonctionnalités telles le partage de l'accès à Internet ou la capacité d'opérer un VPN ou un service de téléphonie IP. Notons que dans un arrêté récent [77], le CRTC a décidé de la fin de ces pratiques, effectif en fin 2017. Ensuite, *Apple* doit beaucoup de son succès à sa plateforme musicale *iTunes*, de laquelle découle un incitatif pour *Apple* à protéger le contenu à propriété intellectuelle au travers des DRMs. On décèle clairement l'influence du modèle d'affaires sur le rôle des utilisateurs dans la conception de ce produit. Le téléphone comporte donc d'importants mécanismes afin de restreindre la capacité d'exportation de parties de son contenu. Philosophiquement et d'un point de vue du management, ce ne sont pas des éléments qui favorisent le développement d'une culture d'ouverture, de liberté et de respect des droits des UFs. Cela justifie des décisions architecturales telles le « *(soft-) sandboxing* » au niveau des applications.

À l'inverse, Google a agi [80] d'un point de vue façonné à la fois par son histoire [81] et par la situation du moment, lequel penchait davantage vers l'ouverture, et décida donc d'une approche plus libre, mais encore. Dans l'absolu, les utilisateurs opèrent sur une plateforme mobile à code source ouvert, mais cela prit quelques années avant que tout le code soit ouvert (une partie de cela était du fait de Sun, ayant des droits sur Java, et appartenant de nos jours à

Oracle) [64] . Encore aujourd'hui, même si le code source est ouvert et que, en théorie, les utilisateurs peuvent utiliser les services d'un compétiteur de Google, il faut aller dans des versions alternatives (« *mods* ») un peu obscures tels *Cyanogen Mod*, afin de vraiment opérer sans être constamment, quotidiennement, voire plusieurs fois par jour, sur le radar de l'OP, Google. Au stade actuel, Google jouit essentiellement de la première position en termes d'adoption de son OS mobile [82], et du fait de cet ensemble d'utilisateurs, la très vaste majorité est sur une plateforme originale, sur laquelle Google détient le leadership dans le développement et qui est très intégrée avec ses autres services. Bref, tout Google réussit à influencer [83 et 84], pour ne pas dire dicter, les éléments essentiels dans la conception logicielle [85]. Cela arrive également du côté du matériel des appareils mobiles, où Google occupe une position de leadership auprès de la « *Open Handset Alliance, (OHA)* ». Ce faisant, l'idée à garder à l'esprit est que les compagnies oligopolistiques dans ce domaine se prêtent à un exercice d'ouverture contrôlée lorsqu'elles ont besoin d'apports ou de contributions qui leur échappent. Ces apports peuvent être par exemple, le développement d'applications, la compatibilité avec d'autres normes ou produits mieux implantés (ex : les gestionnaires d'appareils mobiles, voir section [S: 1.2], le développement de produits accessoires (ex : les bidouilleurs ou « *makers* » et tous les bidules qu'ils bricolent) ou simplement l'adoption d'un produit vers un concurrent supérieur à quelque égard que ce soit. Du côté de Google, le modèle d'affaires est basé sur la publicité, qui se veut ciblée, et de ce fait, sur la qualité de la connaissance qu'a Google de l'utilisateur. Encore une fois, le modèle d'affaire, plutôt que les besoins des utilisateurs, définissent les caractéristiques du logiciel.

En somme, tel que détaillé plus haut, il semblerait que ces épisodes d'ouverture soient généralement contraires aux intérêts d'affaires des OPs et que ceux-ci n'y cèdent qu'à reculons, tout en s'affichant grandement motivés et préoccupés par les libertés des utilisateurs, avec des discours parfois grandiloquents [86] . Aux intérêts commerciaux des opérateurs de plateforme s'ajoutent ceux de divers agents étatiques, des développeurs d'applications et d'intergiciels, mais toujours pas ceux des UFs. Ainsi, la totalité de l'étendue de la liberté des UFs se résume et se limite à opter parmi les choix proposés, mais ne s'étend pas à la capacité d'élaborer ces choix où à en influence le façonnement.

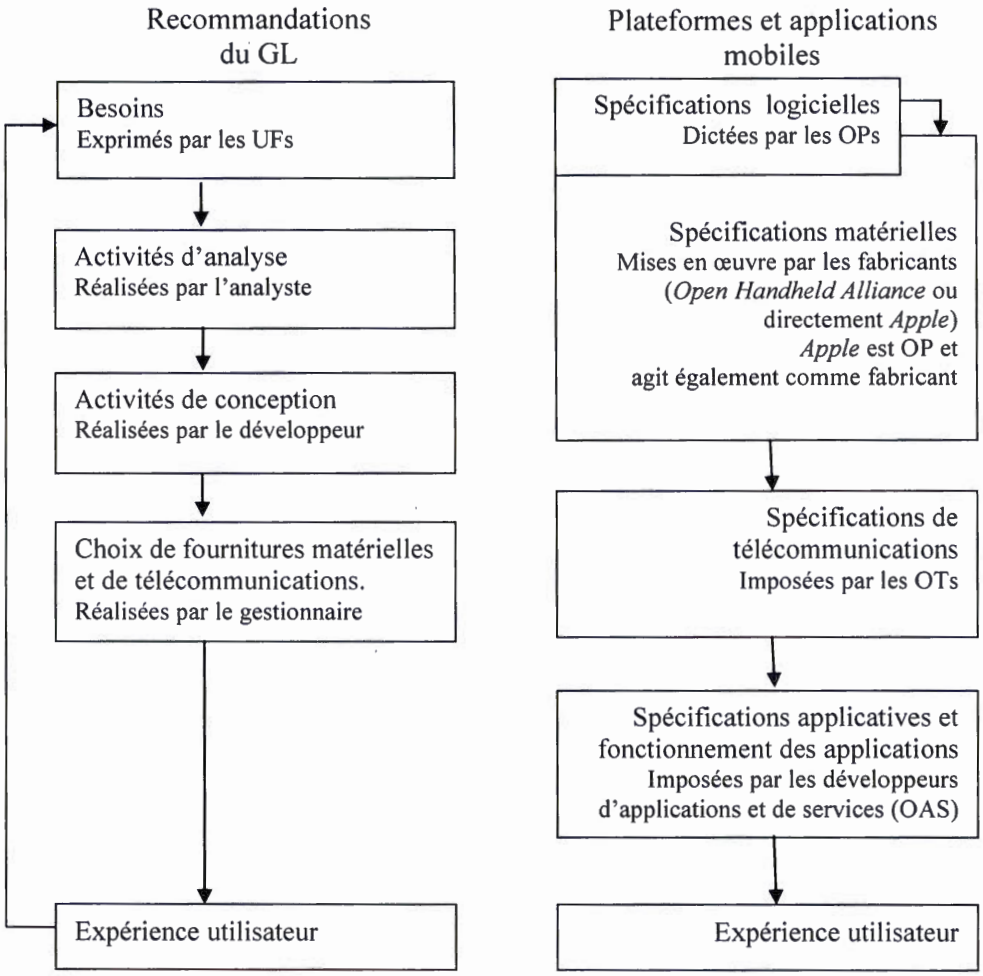
Or, tout espoir n'est pas perdu, sinon la présente discussion serait totalement vaine. L'évolution dépend parfois d'un concours de circonstances, principalement ces circonstances sont en fait le développement de technologies nécessaires à cette évolution ou l'assouplissement de certaines règles ou influences, ou encore, des tendances ponctuelles ou de fond qui motivent des changements de comportement chez les utilisateurs. Ensuite, la notion de responsabilité individuelle mentionnée antérieurement revient sous le fait de saisir ou non cette opportunité d'évolution. Les problèmes inhérents à la GIDIM classique se font ressentir, parfois de manière assez pressante et l'industrie réagit. Notamment, le contrôle sur les données par les OPs est un frein à l'adoption en entreprise, sur trame géopolitique, et certains fabricants, comme Samsung, répliquent en présentant des solutions, telles Knox. Pour l'instant, celles-ci constituent une première évolution à partir du fonctionnement original en matière de GIDIM, mais cette alternative sert principalement les intérêts des employeurs des UFs et non des UFs eux-mêmes, en tant que personnes.

Le présent mémoire fait état d'une prise de conscience d'une part importante des UFs face à leurs données, de l'existence de normes neutres, ouvertes et/ou internationales en matière de GIDIM, ainsi que de technologies nécessaires pour qu'il soit possible pour les utilisateurs d'évoluer vers un logiciel dont la conception prend en compte leurs besoins, ou du moins tend vers cette préoccupation, puisque ces besoins et la conscience même de ces besoins peut différer grandement d'un utilisateur à un autre.

1.4 Le génie logiciel à la rescousse

Normalement, les meilleures pratiques en matière de génie logiciel requièrent qu'à l'étape de l'analyse, les besoins des parties prenantes soient élicités [87 et 88]. D'ordinaire, une grande importance est conférée aux exigences telles qu'élicitées par les utilisateurs. La plupart des modèles modernes du cycle de vie (et du développement) du logiciel, pour des logiciels de cette importance (il est question du système d'exploitation duquel dépendent des milliards d'appareils mobiles) ont des aspects itératifs et incrémentaux, mais l'importance d'une analyse adéquate des besoins est préservée. Or, en matière de technologies mobiles, les besoins exprimés par les utilisateurs sont absents à plusieurs égards. Certes, les considérations

d'ergonomie par groupes de discussion (« *focus groups* ») laissent aux utilisateurs une grande voix au chapitre. Or, il y a quelques domaines où leur perspective a beaucoup moins de poids : la gestion de l'identité des individus, la gestion des données, la gestion des coûts, la gestion de la vie privée, la durabilité des appareils, l'universalité et la portabilité des profils, etc. Tous ces domaines ont en commun le fait que les intérêts des utilisateurs sont en conflit avec ceux d'acteurs plus puissants, notamment les opérateurs de plateformes ou de télécommunications, ainsi que les développeurs d'applications.



Légende :

⟶ : Sens de l'influence dominante

Figure 1.3 – Comparaison des modèles d'influence lors du développement de logiciels (entre les meilleures pratique recommandées par le GL et les observations en matière de développement de plateformes et applications mobiles).

Devant la difficulté de contrôler le développement de l'évolution des technologies grand-public, le caractère ouvert de certaines plateformes a donné lieu au développement d'alternatives et d'extensions spécialisées ainsi qu'à la migration de segments de la population d'utilisateurs vers des technologies autres, orientées vers une gestion (GIDIM) beaucoup plus défensive et bien connues par divers profils d'utilisateurs, dont les cybercriminels. Cela a un impact sur la capacité de l'État a exercer certaines de ses fonctions régaliennes. Bref, à force de ne pas répondre à ce besoin, on voit poindre une migration vers des zones virtuelles de non-droit, les phénomènes du *DeepWeb* et du *Bitcoin* vont un peu dans ce sens. Une situation inadéquate où la confiance entre les institutions est minée, et qui mène à l'adoption massive de voies alternatives, porte atteinte à la sécurité du plus grand nombre qui est nécessaire au développement de toute société de droit libre et démocratique. Par conséquent, un exercice qui viserait à éviter ces débordements et ces migrations vers des plateformes souterraines, serait d'une grande importance sociale. Cela requiert de s'assurer que la situation actuelle, telle qu'observée par le plus grand nombre, ne soit ni inacceptable, ni abusive au regard des intérêts des utilisateurs, et de combler tout écart découvert.

En l'espèce, il s'agit d'un travail de recherche novateur puisqu'il se base sur une approche principalement inspirée de la partie « élicitation des exigences » de la méthodologie du génie logiciel, mais toute la dimension des politiques d'utilisation et des contraintes de gouvernance revêt un aspect social et juridique puisque c'est la loi, sous ses diverses formes (législation, jurisprudence, doctrine, etc.) qui codifie ces contraintes opérationnelles. Le génie logiciel aplatit les contradictions, formalise les ambigüités. Ainsi, le GL propose un *comment*, laissant le *quoi* libre. On ne cherche pas ici à combler un déficit de conception dans les systèmes d'exploitation mobiles, on cherche à s'implanter très tôt dans le développement d'une nouvelle sorte d'approche envers l'informatique personnelle et dont le cas de figure étudié est celui des appareils mobiles. Cela est tel pour des questions de circonstances, mais les préceptes peuvent être généralisés. L'espoir des mouvements de défense des droits des utilisateurs à la fin de la section historique [S : 1.3] et l'évolution décrite subséquemment prend racine dans la maturation actuelle de l'informatique personnelle, telle qu'elle existe présentement dans nos appareils mobiles. Elle s'inscrit en anticipation de l'Internet des Objets, et d'autres évolutions similaires, en prenant assomption à l'effet que tous ces objets connectés et personnels utiliseront probablement le téléphone mobile comme point de

jonction. Aussi, toujours dans l'anticipation, la perspective dans laquelle est produit le présent mémoire se conforme aux tendances de dématérialisation qui sont observées. Ainsi, les changements proposés font du téléphone mobile un simple point d'accès ou de jonction, animé par un système qui lui permet, moyennant les authentifications appropriées, d'accéder à l'une ou l'autre des identités, et de permettre à l'utilisateur de les exercer. Ce sont les besoins des utilisateurs face à ce système qui seront modélisés. Évidemment, cette modélisation se basera grandement sur l'état actuel des choses, lequel se base sur une conception du téléphone mobile qui se rapproche de « l'extension du soi » [89, 90, 91 et 92], pour migrer vers une extension générique que l'on peut s'approprier, mais qui est régie par une sorte « d'autre soi », qui nous permet de gérer notre identité sur plusieurs points de contact, qui seront de fait, principalement mobiles. Le présent mémoire ne détaillera pas tous les changements nécessaires à cette fin, telle n'est pas sa portée. Il se concentre sur les changements qui doivent être apportés au modèle actuel en matière de besoins afin de permettre ces extensions. Tout au plus, il y aura quelques exemples de mises en œuvre.

Par exemple, de nos jours, lorsque l'on conduit, si notre véhicule est équipé avec Bluetooth et que l'on désire apparier notre téléphone avec notre véhicule, notre tableau de bord copie nos contacts et interagit avec notre cellulaire pour gérer les appels. Or, dans les versions plus anciennes de véhicules ainsi que dans certaines versions récentes, si on loue ou on emprunte une voiture, il faut effacer les données transférées au tableau de bord afin d'éviter que le prochain utilisateur n'y accède. Or, s'il y avait un système de GIDIM normalisé, celui-ci pourrait être commun pour le téléphone ou le véhicule et cette chaîne de points de contact pourrait être gérée de manière transparente. Le téléphone pourrait déployer l'identité sur le tableau de bord, après authentification des parties et seulement pour le temps nécessaire. Cela pourrait aussi fonctionner sans égard au fait qu'un point de contact (dispositif servant d'interface entre l'UF et le système) soit sous plateforme *iOS* et l'autre sous plateforme *Android* ou quelque autre plateforme que ce soit. La même approche pourrait être observée pour tout autre appareil intelligent : frigo, guichet automatique, portes d'accès, panneau domotique, etc. Une fois les principes établis, la matérialisation peut prendre diverses formes. Par exemple, dans le cas d'un système domotique, nul besoin d'un écran pour entrer un identifiant et un mot de passe, il suffit de donner un court identifiant unique, peut-être dix caractères, qu'il soit permanent ou temporaire, puis l'authentification pourrait se faire par la

voix, toujours selon le principe d'identité portable. Cette idée d'identité portable, qui doit être gérée, mène, à terme, au concept d'assistant virtuel, au sens abstrait, soit un ensemble de logiciels qui sont coordonnées selon les besoins d'un UF et qui interagissent avec divers autres systèmes pour agir au nom de celui-ci. Dans un contexte d'automatisation, cet assistant virtuel confère un avantage concurrentiel : il est capable de suivre le pas des autres systèmes automatisés, plus rapides que le plus rapide des assistants humains, et capable d'opérer des négociations complexes, de participer à des enchères automatisées, d'effectuer des routines chronophages (e.g. : télécharger les nouvelles des balados programmées, sélectionner les nouvelles les plus pertinentes sur les médias sociaux plutôt que de laisser *Facebook* le faire pour nous, etc.), etc. Cette idée d'assistant virtuel requiert par son essence même que les besoins des utilisateurs soient un élément prioritaire, que ceux-ci soient bien élicités et bien modélisés. Encore une fois, attendu qu'il faut circonscrire le travail de recherche, le sujet de l'assistant virtuel ne sera ici qu'effleuré.

1.5 Présent document

Le présent document se veut un travail de recherche qui s'inscrit dans le mémoire pour l'obtention d'une Maîtrise en informatique de gestion, auprès de l'Université du Québec à Montréal. Pour ce motif, il doit répondre à certains critères bien précis, tant sur le fond que sur la forme. Or, le présent mémoire puise sur des recherches [93, 94, 95, 96, 97, 98 et 99] en continu qui vont, semaine après semaine, de 2005 à 2017, soit de l'étude de première main d'un entrepreneur et chercheur dans ce domaine tout au long d'une période allant de l'aube de l'ère des téléphones intelligents au moment actuel. À sa base même, le but de ce mémoire est d'illustrer une transition entre un état initial insatisfaisant et un état proposé jugé meilleur, puis de détailler et justifier ladite transition. Autant que se peut, le style de citation retenu sera celui de l'IEEE pointant vers une référence présentée en format APA (« *American Psychiatry Association* »), tel que requis par le GuideMT 2.0, suivi d'une note de référence.

1.6 Cadre conceptuel

Cette section et ses sous-sections permettent de situer l'activité de recherche documentée par le présent mémoire à l'intérieur des activités précédentes effectuées dans cette voie, tant par le chercheur actuel que par les chercheurs précédents. Elle permet d'énoncer la problématique de recherche, de poser le sujet de recherche et de mettre le livrable en contexte.

1.6.1 Sujet

Le sujet des besoins des UF en matière de GIDIM s'inscrit dans le cadre d'une des grandes étapes identifiées [88] par le GL, soit l'analyse des besoins, étape première de la plupart des méthodologies reconnues en génie pour le développement de ces logiciels. Cela implique d'abord de connaître les besoins en matière de GIDIM qui demeurent à combler malgré les récents développements en la matière, notamment celui d'initiatives spécialisées telles Samsung Knox [100] qui servira de point de départ. Cela requiert également de documenter ce qui se fait actuellement en la matière ainsi que répertorier les principales sources qui recensent ces besoins ainsi que les principaux enjeux en la matière. Cette perspective se centre sur les enjeux au Québec, mais s'étend aux enjeux ailleurs dans le monde, dans la mesure où ceux-ci sont toujours pertinents dans le contexte du Québec.

1.6.2 Problématique

Toute activité de recherche vise à obtenir de la connaissance valable afin de répondre à une question, celle-ci permettant généralement de résoudre un problème. La réflexion sur la problématique de recherche permet de définir le problème à l'étude, d'en décrire l'impact et d'en justifier la pertinence. La définition du problème permet de circonscrire l'activité de recherche et d'éviter les débordements et l'allocation sous-optimale des ressources de recherche; l'impact permet de contextualiser l'activité de recherche et la justification permet

d'assurer une proportionnalité entre les moyens investis pour l'effort de recherche et les bénéfices espérés. En l'espèce, la problématique est celle de la non-représentation des besoins des utilisateurs en matière de GIDIM.

Définitions du problème et de l'objet à l'étude

Les technologies mobiles font partie intégrante de nos vies et jouent un rôle important dans celles-ci. Or, contrairement aux meilleures pratiques en matière de génie logiciel, leur développement ne se base pas sur les besoins des clients (ceux qui paient, les UFs), mais sur les décisions opérationnelles, techniques et stratégiques de divers autres acteurs, principalement les opérateurs de plateformes et de réseaux, les développeurs d'applications, ainsi que les fabricants des appareils. Ceux-ci sont organisés et bien que rivaux, ils sont des décideurs *de facto* des modes d'opération auxquels les utilisateurs doivent se conformer. Cet écart entre les besoins des utilisateurs et les orientations des décideurs sont un espace où viennent se nicher des technologies dérivées spécialisées qui voient dans celui-ci une opportunité d'affaires. Malgré cela, ces initiatives, il reste encore des améliorations à apporter et le présent mémoire vise à proposer un modèle qui répondrait aux besoins qui demeurent non-comblés. De manière connexe, à ce stade, il serait utile définir formellement l'objet conceptuel de l'étude du modèles de modes d'opération comme étant celle des facteurs utiles à l'élaboration d'une diversité comparée de groupements de caractéristiques techniques et opérationnelles associées à des groupes de besoins circonstanciels d'utilisation des technologies de GIDIM.

Description de l'impact de la problématique

L'impact de ces besoins non-comblés est important et diversifié. Il touche essentiellement les libertés civiles ainsi que l'efficacité des moyens collectifs que les citoyens se sont donnés pour façonner les institutions qui régulent plusieurs aspects de leurs sociétés. Par ailleurs, en réaction à cela, une frange de la population d'utilisateurs migre vers des plateformes d'anonymat, ou plus précisément de pseudonymie complète, et qui sont bien connues de

divers groupes, dont des cyber-délinquants. Même pour ceux qui adhèrent aux modèles de base proposés, il y a des implications importantes, notamment en ce qui a trait à l'influence qui est conférée à des acteurs privés et commerciaux (à but lucratif). Par exemple, en vertu de leur liberté contractuelle [101], ceux-ci peuvent refuser l'accès à leur plateforme à qui bon leur semble. En considérant que des activités essentielles à la vie sociale, telles le paiement des impôts, le commerce et l'obtention de services gouvernementaux, basculent vers des guichets ou des interfaces qui rendent obligatoire l'adoption de TIC privées, dont les technologies mobiles sont un composant important, c'est la viabilité et la légalité de la transition vers ces stades imminents de l'évolution de la vie sociale qui peuvent être compromises tant par l'influence conférée aux acteurs privés et commerciaux que par les risques résultants de la désadhésion vis-à-vis un terrain commun de confiance nécessaire à ces interactions sociales.

Justification de la problématique

Il y a un écart très important entre les intérêts des utilisateurs et les intérêts des décideurs. Parfois, ces écarts peuvent se justifier, d'autres fois non et c'est ce qui semble être le cas en l'espèce. Ces écarts s'inscrivent d'ailleurs dans une tendance générale d'érosion des libertés publiques [102, 103 et 104] qui semble liée à la croissance de l'utilisation des TIC en absence d'encadrement adéquat de celles-ci. Plusieurs groupes s'inquiètent de cette tendance, expliquent pourquoi elle est problématique et proposent des pistes de solution[105]. Cette tendance est grave du fait qu'elle rend possibles et même hautement plausibles, divers abus qui sont contraires à certaines règles fondamentales [106] sur lesquelles reposent des pans entiers des normes qui régissent la société de droit que les citoyens actuels, et les générations précédentes, ont âprement bâtie. Il est essentiel de proposer des alternatives responsables [107, 108 et 109] parce que de plus en plus d'aspects de notre vie se basent sur les technologies mobiles et cette perte de libertés a des conséquences qui fragilisent les individus et qui, à terme, menacent la paix sociale.

Par exemple, les modèles d'affaires actuels de plusieurs services qui apparaissent aujourd'hui comme essentiels reposent sur un financement à partir des revenus publicitaires qui sont

optimisés sur la base de données recueillies et traitées. Cela requiert une confiance mutuelle entre les opérateurs et les utilisateurs. Or, si suffisamment d'utilisateurs délaissent le service ou l'emploient de manière dégénérée, par exemple, au travers de l'utilisation d'obfuscateurs ou de bloqueurs publicitaires, c'est la rentabilité et la viabilité de ces modèles d'affaires qui peut être compromise.

Un autre exemple peut être celui des finances en ligne. Si un profil d'utilisateur veut effectuer des achats qui peuvent être légaux (ou non), mais qu'il refuse que ce genre d'achats puisse être imputé à son dossier à cause des conséquences néfastes (et qu'il perçoit peut-être comme injustes) qui s'y rattachent, il se peut qu'il privilégie une plateforme qui lui garantit cette sécation, l'isolement de type d'achats, quitte à qu'elle soit mal famée ou tenue par le crime organisé. Cela s'inscrit dans une logique de contournement de certains monopoles d'État, tels le jeu [110] ou l'alcool. Dans la réalité concrète, l'achat régulier d'alcool ou de jeux par carte de crédit attitrée peut avoir une influence négative sur la cote de crédit [113, 114, 115 et 116] dans certaines juridictions. Cela peut justifier, chez certains utilisateurs, de se tourner vers des alternatives informelles. C'est un exemple typique de cas où l'incapacité de répondre à certains besoins peut avoir plusieurs conséquences. En l'espèce, elle peut favoriser le crime organisé, exercer une concurrence déloyale à l'encontre des monopoles d'État, exposer l'utilisateur à des risques importants de fraude et contribuer au financement et à la volumétrie d'activités criminelles ou dont la légalité demeure indéterminée, le tout en marge de la capacité de l'État à percevoir des revenus issus de la taxation ou l'opération de ces activités et à endiguer la consommation problématique[117 et 118].

1.7 Objectifs de recherche et question de recherche

L'objectif de recherche est d'élaborer un modèle de modes d'opération qui résorbe encore davantage l'écart entre le modèle de besoins et les modes d'opérations existants, au-delà de Knox. Bref, il s'agit d'une amélioration d'un modèle existant sur la base d'un ensemble de facteurs qui seront recensés et organisés par l'activité de recherche.

La question de recherche peut se formuler comme suit : « Au-delèa de Knox, quel apports nouveaux peuvent être apportés aux modèles de modes d'opération existant en matière de GIDIM? »

Notons par ailleurs que le contexte dans lequel se situe la question de recherche est très complexe et qu'il foisonne d'enjeux et de questions de recherche valables. De plus, plusieurs de ces questions donnent ouverture à nombre d'autres questions pertinentes. Il est donc impératif de garder le cap sur une seule question et de bien délimiter la portée de celle-ci, avec le degré juste de couverture des enjeux connexes, sans toutefois déborder.

1.8 Notes sur le livrable

Le livrable est un modèle de modes d'opérations et d'autres améliorations connexes rassemblant l'intégration la plus complète des apports qui auront été trouvés, en regard du modèle des besoins qui auront été recensés par la revue de la littérature.

1.9 Structure du document

Ce mémoire comprend, outre l'introduction en guise de premier chapitre, une revue de la littérature qui illustre les premières itérations de recherche documentaire, permettant d'acquérir plusieurs concepts à la suite de l'étude et qui sont regroupées au second chapitre. Suit le troisième chapitre portant sur la méthodologie employée. Puis, suit la section présentant les résultats, itérativement tout au long de ce quatrième chapitre, lequel comprend également les discussions et analyses se rapportant auxdits résultats. Enfin, le tout est clos par un bref cinquième chapitre présentant la conclusion de la présente étude.

CHAPITRE II

REVUE DE LA LITTÉRATURE

La revue de la littérature constitue une partie importante de tout travail de recherche. D'ordinaire, il ne vise qu'à recenser l'état de la science actuelle sur le sujet, principalement afin de s'assurer de bâtir strictement au-delà. Or, attendu que la présente activité de recherche comporte un volet documentaire important, il aurait été possible de présenter les connaissances trouvées par l'activité de recherche documentaire, aussi bien dans les sections appartenant au chapitre de la revue de la littérature, que dans une certaine mesure, dans celles appartenant à celui de la présentation des résultats. En l'espèce, les connaissances antérieures à l'élaboration de modes d'opération se trouveront dans la section « revue de la littérature » et la section vouée aux résultats visera à présenter le plus fluidement les modes élaborés, le tout à partir des éléments trouvés dans la littérature, ainsi que certains résultats très saillants. Il y a donc une structure pyramidale dans la présentation des résultats, principalement afin de faciliter la synthèse des connaissances.

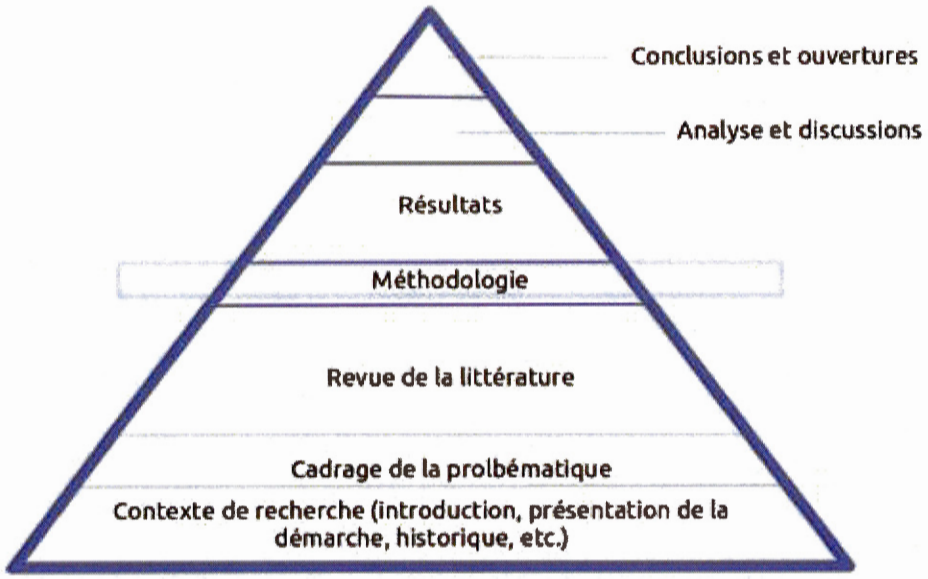


Figure 2.1 – Pyramide volumétrique de l'expression de la présente recherche

2.1 Stratégie de travail et présentation de la séquence de travail (*a priori*), relative à la revue de la littérature

La revue de la littérature pour cerner et étudier cette problématique doit se faire en plusieurs étapes successives, les unes servant à la compréhension des étapes suivantes. Ces étapes se regroupent en des phases.

Il y a d'abord les phases d'étude de la littérature antécédentes à la problématique.

- Premièrement, il faut définir ce que sont les données personnelles et les données d'identité.
- Ensuite, il faut présenter comment sont traitées ces données dans divers cadres opérationnels, réglementaires ou législatifs.
- Puis, il faut attribuer des valeurs à ces informations. Pour ce faire, il faut éliciter les incitatifs des parties impliquées et les enjeux.

En deuxième lieu, vient la phase ciblant de spécifiquement la problématique visée.

- La première composante de cette phase est la description technique des deux principales plateformes et de leur évolution.
- Le deuxième élément de cette phase de la revue de la littérature est la description des modèles de gestion de l'identité sur plateforme mobile : valeur, transférabilité, politiques, etc.
- Le troisième volet de cette phase est le plus costaud et il concerne l'inadéquation de ces modèles, c'est-à-dire, l'ensemble des critiques formulées à leur égard.
- Il se divise en deux sous-volets : les critiques politiques et les critiques techniques.
- Le quatrième et dernier volet documente les améliorations existantes.
- Chacune de ces étapes sera documentée de manière plutôt chronologique.

L'étude de la littérature se constitue des éléments textuels, ainsi que d'autres médias qui se rapportent à l'un ou l'autre des éléments nécessaires à la recherche du sujet de l'étude, pourvu que ces sources soient généralement accessibles, stables et que leurs auteurs soient connus. En

ce qui concerne les aspects techniques, les sources privilégiées sont les articles révisés par les pairs, suivis des résumés de conférences, puis des monographies, de la littérature gouvernementale, de la littérature technique provenant de l'industrie (à n'être considérée qu'au chapitre de ses éléments factuels ou techniques), puis de celle émanant de toute autre source (généralement sous réserve que la méthode soit documentée et que les activités soient reproductibles). Au chapitre des aspects politiques, la source privilégie sera la législation, suivie de la jurisprudence, puis de la doctrine (incluant les articles de recherche juridique), les études de droit comparé, les communications gouvernementales et, enfin, les communications politiques (partisanes ou non, généralement, sous condition que leurs auteurs soient connus ou attribués). Le recensement des documents concernant les modèles et la méthodologie sera contenu dans la troisième section (méthodologie). Pareillement, les considérations relatives à la pondération des sources seront abordées également à cette section.

2.2 Étude de la littérature initiale

La présente section et ses sous-sections présentent la couverture que fait la littérature de concepts, enjeux et autres considérations qu'il est nécessaire d'aborder avant d'aborder la problématique des besoins en matière de GIDIM. Le sujet étant pointu, le respect de cette règle d'antécédent permet de s'assurer que la discussion porte sur une base commune, notamment sur le corpus général et technique ainsi que sur le cadre normatif. Elle permet également l'adoption d'un vocabulaire normalisé et s'inscrit dans l'objectif général de toute revue de la littérature : concentrer les efforts de recherche sur les aspects novateurs, qui demeurent inconnus, et éviter de trop s'attarder, en absence de justification, sur l'étude d'éléments ayant déjà été couverts et faisant consensus.

2.2.1 L'identité des individus

Le concept d'identité en est un philosophique. Par conséquent, il n'existe pas de définition absolue de ce concept. Ce concept est tellement important en philosophie et en cognition, qu'il est axiomatique, il fait l'objet de définitions circulaires. Il existe cependant diverses

définitions formelles et utiles de ce concept. Formellement, la *Stanford Encyclopedia of Philosophy* [119] divise l'identité entre l'identité qualitative et l'identité quantitative, seule la seconde étant absolue. L'identité peut avoir un sens mathématique, lequel peut être utile en logique des prédicats, notamment lorsqu'il est question, dans un système informatique, de confirmer l'identité d'un individu. Or, la compréhension ordinaire du concept, se rapproche de celle proposée par l'Encyclopédie Larousse :

> « Caractère permanent et fondamental de quelqu'un, d'un groupe, qui fait son individualité, sa singularité » [120].

Or, l'identité n'est pas propre aux individus, elle peut également s'appliquer aux groupes d'individus, aux institutions, à des systèmes informatiques, à des amas de données et à d'autres entités. L'identité se rattache normalement à un individu, un seul à la fois et généralement de manière permanente ou continue, mais pas toujours. Il y a une importante incidence de l'attribution non-exclusive entre individus et identités et celles-ci peuvent, dépendamment des contextes, relever du personnage, de l'usurpation ou de la fraude. Aussi, à mesure que l'informatique évolue, les lignes entre l'organique et l'artificiel peuvent se confondre et il devient de plus en plus important de bien cibler. Il faut également noter que l'ensemble des caractéristiques évolue, donc l'identité est aussi dynamique. Ce qui demeure constant dans le concept d'identité, c'est qu'il s'agit d'un ensemble non-nul d'attributs qui permettent d'effectuer une distinction entre un élément d'un groupe et (tous) les (autres) éléments de celui-ci. Cette propriété fait de l'identité un concept relatif et téléologique, c'est-à-dire que l'identité n'est pas une finalité en soi, et qu'elle requiert obligatoirement un ensemble, en l'absence duquel elle est dépourvue d'utilité, voire de sens. Lorsque l'on rapporte ces considérations aux individus, cela donne un caractère fondamentalement social et utilitaire à ce concept. L'identité rattache l'individu à la société, elle est la base de l'interaction sociale, et elle sert également de socle pour d'autres processus utilitaires tels l'imputation et l'exercice des droits et devoirs, dont ceux de propriété, de détermination et de solidarité. Ces caractères fondamentaux sont transposés, volontairement ou non, dans les modèles informatiques de divers systèmes (dont les technologies mobiles), avec lesquels les utilisateurs interagissent et qui régissent de plus en plus leurs vies.

2.2.2 Les données personnelles

Les utilisateurs produisent, de manière continue, des volumes importants de données. L'existence et les propriétés physiques peuvent être exprimées en des volumes assez restreints de données, un octet pour la taille au centimètre près, 4 bits pour la couleur des yeux, deux octets pour le poids à la demie-livre près et 64 bits pour notre position géographique au mètre près sur la surface du globe. Cette simplicité rend possible l'agréation de quantités importantes de données, même avec des dispositifs aux ressources limitées (de connectivité et de stockage) tels les appareils mobiles. Cela fait de ce genre d'appareil un objet de choix pour procéder à ces collectes en continu, en temps réel; de là l'importance de bien encadrer ces activités sur ces appareils. Ensuite, il faut savoir que données personnelles ne sont pas nécessairement toutes des données de GIDIM, mais elles peuvent le devenir si elles servent à des activités de gestion de l'identité, principalement d'authentification et de profilage, d'élaboration de l'identité et du patrimoine informationnel des individus.

2.2.3 Les données d'identité, la gestion de l'identité et les enjeux et besoins qui s'y rattachent

Depuis ses débuts, l'informatique de gestion est une activité qui, par sa nature s'est poursuivie au support de technologies et qui a quelque chose d'inhérent cherchant à s'extraire de l'égalité et ce dans un degré important, au-delà de ce que la simplement organisation hiérarchique permet, le rapport recherché se veut virtuellement illimité. Il y a là quelque chose d'intrinsèquement proche de la notion de contrôle (des masses). Cela n'implique pas nécessairement de mauvaises intentions, mais il faut reconnaître certains corrélaires à cette rupture avec l'égalité et ses principes.

De manière concrète, il n'y a pas de négociation ou d'accord de gré-à-gré, il est question d'un rapport d'adhésion (volontaire ou pas) au sens juridique du terme. L'opérateur dispose d'un actif (technologique) qui lui confère la capacité d'induire un rapport de force avec un nombre illimité d'individus, lesquels doivent s'organiser pour rééquilibrer les forces. Toutes ces notions qui peuvent sembler politiques ou philosophiques se répercutent dans des aspects très

concrets en matière d'applications mobiles. Par exemple, dans une relation dépersonnalisée, il n'y a pas de possibilité de se fier sur le fait qu'il connaisse l'opérateur de la plateforme. Il faut se fier, soit aux données historiques conservées, ou à une autorité externe reconnue comme compétente. Or, de plus en plus, d'autres options émergent au fil que les technologies et leur usage se développe. Enfin, l'efficacité à gérer des volumes importants de données permet la mise à l'échelle d'un système et cela a également une influence sur le modèle d'affaires. Une grande partie des systèmes les plus populaires basent leurs modèles d'affaires sur la gratuité du service contre une exposition publicitaire, laquelle ne peut être rentable que si le nombre d'utilisateurs est important. Dans ce cas, c'est la viabilité même du modèle qui dépend de la capacité de la technologie à gérer un rapport dirigé avec un bassin quasi-illimité d'utilisateurs. Le modèle a besoin que le service soit dépersonnalisé et l'utilisateur, petit.

L'identification peut être réclamative ou attributive. Dans le premier cas, quelqu'un se réclame d'une identité, il revendique une référence d'interaction avec le groupe : « je suis Normand ». Dans le deuxième cas, quelqu'un propose d'associer une entité à un référentiel : « c'est Normand ». La première approche est la plus commune, c'est ce que l'utilisateur fait quand il entre son nom d'utilisateur. La seconde approche est celle qui est généralement utilisée dans une démarche judiciaire, de gigadonnées ou de reconnaissance biométrique : on conclut que c'est Normand, qu'il l'ait demandé ou pas Dans les deux cas, il s'agit de produire un réseau, plus ou moins complexe, d'inférences, depuis les senseurs qui procèdent à la capture brute de données, et qui permet de remonter jusqu'à la déclaration que celles-ci cherchent à valider. L'identification est donc une conclusion par réseaux de propositions.

Par exemple, dans un réseau très simple, il existe une hypothèse, à l'effet que le fait de posséder le mot de passe suffise à prouver l'identité. L'utilisateur, en fournissant son nom d'utilisateur et son mot de passe, permet de compléter le graphe nécessaire à l'identification, CQFD. Les cas d'identification attributive sont plus complexes. Des éléments comportementaux peuvent avoir des contributions pondérées au graphe, lequel peut être satisfait uniquement après que plusieurs conditions cumulées soient rencontrées. L'identité peut également être probabiliste, elle peut être exprimée avec des degrés, sous la forme d'une paire d'intervalles de confiance (méthode Neyman-Pearson [121]).

Dans les cas d'identification réclamative, le processus de complétion du graphe permettant de d'arriver à la conclusion d'identification s'appelle l'authentification. Ce terme est choisi puisqu'il est question d'un processus permettant de déterminer le caractère authentique d'une affirmation.

La gestion de l'identité ne se limite pas à l'authentification. Il s'agit d'une activité de gestion très riche et diversifiée qui inclut de très nombreuses facettes [122 à 143] : gestion de la vie privée, gestion de la vie publique (réputation et certification), personnalisation des données et des préférences, valorisation et marchandisation des données, protection du droit à l'oubli, exercice des droits et accomplissement des devoirs, portabilité des données, exercice de souveraineté, etc.

Certaines données sont particulièrement importantes dans un contexte mobile et celles-ci sont définies par les capacités offertes par les appareils mobiles. Notamment, les capteurs audio, vidéo et GPS, ainsi que les capacités de communications qui sont propres aux téléphones intelligents, font des données suivantes des données importantes en matière de GIDIM : photos et vidéos, enregistrements sonores, appels, messages, emplacement et historique de navigation et déplacements [145 à 149].

Il est difficile de prendre un instantané, même dans la littérature, de l'état actuel de la situation, tant l'objet d'étude bouge rapidement. D'une part, le sujet de la gestion de l'identité est recherché par de plus en plus de chercheurs. D'autre part, celui-ci dépend d'une réalité qui est en pleine mutation, celle de la base matérielle de l'offre de services. Ainsi, le fait que l'ensemble de l'expérience numérique soit en train de migrer vers une base infonuagique change de manière importante les paradigmes, notamment ceux en matière de GIDI(M).

Les principaux besoins en matière de GIDI, tels que recensés dans la littérature, sont les suivants :

1) permettre l'authentification, de laquelle découle la gestion des accès (depuis Quisquater ou Günther [150, 151 et 152], en 1990, jusqu'à aujourd'hui).
2) permettre de développer un patrimoine numérique (« *digital legacy* », de Paul-Choudhury, 2011) [153].
3) permettre l'exercice des composants de son identité (rôles, interactions sociales, droits et obligations, Chowdhury et Noll, dès 2007) [154 à 157]
4) participer à la souveraineté informationnelle de sa nation (« *data sovereignty* », selon Peterson, 2011; Irion, 2012 et Polatin-Ruben & Wright, 2014) [159 à 165] ou de sa communauté.

Ces éléments saillants seront intégrés au chapitre des résultats.

2.3 Concepts mis de l'avant dans la littérature et antécédents à la compréhension des modes d'opération en matière de GIDIM

Cette section présente divers concepts qui reviennent dans la littérature et dont la compréhension est nécessaire à suivre l'élaboration des résultats.

2.3.1 Contrôle d'accès discrétionnaire (« *Discretionnary Access Control* »)

Il s'agit d'un mode de contrôle d'accès où, ordinairement, le « propriétaire » d'une ressource (informationnelle) exerce sa discrétion sur le contrôle des accès à celle-ci. Or, le caractère « localisé » de ce contrôle d'accès pose des limites, par exemple, sur l'incapacité de limiter diverses caractéristiques de l'accès octroyé, notamment la transitivité de celui-ci. Au net, cela mène à des situations où une fois que l'accès est accordé, il ne peut pas être pratiquement révoqué.

2.3.2 Contrôle d'accès obligatoire (« *Mandatory Access Control* »)

Il s'agit d'un mode d'accès plus contrôlé que celui discrétionnaire et qui se base sur des éléments d'un contexte qui est commun à l'ensemble du système. Par exemple, une politique

d'accès peut faire partie d'un tel contexte et cela permet de s'assurer que même si un utilisateur a accès, il ne peut à son tour partager la ressource informationnelle avec un tiers qui n'est pas autorisé par la politique. L'essentiel de la stratégie de durcissement d'*Android* proposée par Smalley se base sur ce mode d'accès. Notons que ce mode est disponible sur Mac OS X [378 et 379] (« *TurstedBSD* »), mais pas sur *iOS*.

2.3.3 Virtualisation

La virtualisation vise l'utilisation d'abstractions de ressources plutôt que les ressources directement. Cette abstraction peut s'opérer à divers niveaux : matériel, système d'exploitation, librairies, intergiciels, applications, etc. Elle vise à assurer un déploiement des niveaux au-dessus de cette abstraction de manière conforme à une spécification et sans avoir à se préoccuper des particularités propres aux ressources qui se trouvent aux niveaux inférieurs. Par exemple, la virtualisation peut être utilisée, dans un contexte mobile, afin de déployer du contenu logiciel au-dessus d'une couche virtuelle minimale permettant de déployer le contenu applicatif de la même manière, sans égard à l'architecture processeur (ARM, x86/*Intel Atom* ou autre) de l'appareil mobile.

2.3.4 Conteneurs

Le concept de conteneurs est présent dans le domaine de l'informatique depuis ses débuts. Il vise la segmentation de ressources de manière à assurer un niveau d'abstraction et de normalisation des couches inférieures afin de pouvoir se concentrer sur une exploitation des couches supérieures pouvant compter sur un niveau normalisé de performance, de requis fonctionnels et non-fonctionnels ainsi que sur des ressources extensibles au besoin. À cet effet, les principales utilisations des conteneurs, de nos jours, sont celles au cœur des serveurs, souvent dans des processus de virtualisation ou de déploiement d'infonuagie, par exemple avec des orchestrateurs tels Kubernetes. Or, la même technologie permet d'avoir des points de contact neutres et de réaliser le parallèle entre les conteneurs mobiles servant à capturer l'instant du moment et les conteneurs en nuage permettant de contenir le patrimoine informationnel de l'utilisateur.

2.3.5 Les couches OSI revisitées

Plusieurs concepts (dont la virtualisation, les conteneurs et les sessions) se réfèrent à une conception de l'utilisation de l'informatique sous une organisation structurelle similaire à celle des couches OSI [380] telles qu'utilisées pour modéliser le transport d'informations par voie de télécommunication, mais s'appliquant cette fois-ci au traitement de l'information plutôt qu'à sa circulation. Ainsi, il y a une couche matérielle qui représente les éléments électroniques sollicités. Au-dessus de celle-ci, en remplacement de la couche liaison (« *link* »), il pourrait y avoir une couche d'abstraction système (kernel), qui joue le rôle d'une base virtualisée et possiblement distribuée (infonuagie) au-dessus de laquelle sont déployés les couches supérieures. La suivante parmi celles-ci serait la couche système, analogue à la couche réseau du modèle OSI et assurant le fonctionnement du système (librairies, coordination, etc.). Le prochain niveau, analogue à la couche transport, serait la couche infrastructure, laquelle intègre les fonctionnalités de qualité de service et de gestion des ressources. Vient ensuite la couche session, laquelle inclut tous les éléments nécessaires à la portabilité de l'utilisation (incluant les sockets et les mécanismes de GIDIM ainsi que les raccordements aux données), puis la couche présentation, laquelle inclut des fonctionnalités de personnalisation et adaptation. Enfin, vient la couche application qui englobe les traitements applicatifs opérés.

Tableau 2.1 – Présentation comparative des couches proposées

#	OSI-Réseau	Traitement	Description
1	Physical	Matériel	Fonctionnalités électroniques
2	Data-link	Noyau/Kernel	Fonctionnalités É/S et virtualisation
3	Network	Système	Librairies et mécanismes contrôle
4	Transport	Infrastructure	Système virtualisé
5	Session	Session	Session d'utilisation
6	Présentation	Présentation	Personnalisation et adaptation
7	Application	Application	Opérations

2.3.6 Carré de sable (« *sandbox* », « *chroot* »)

Il s'agit d'une technique par laquelle les opérations menées sont isolées logiquement du reste du système de façon à ce qu'en cas de compromission, celle-ci ne puisse s'étendre à son ensemble.

2.3.7 Identité en tant que service

Ce concept définit le fait d'offrir un service d'identité, en abstraction des couches inférieures nécessaires au rendu de ce service. Par exemple, ce service doit pouvoir être rendu peu importe que l'élément qui le demande opère sous Microsoft Windows, *Android* ou *iOS*. À ce stade, on peut se concentrer sur des caractéristiques de l'identité tel le niveau de confiance, la volumétrie de portabilité, etc.

2.3.8 Concerteur d'appareils

Il s'agit d'un service logiciel qui permette de concerter les interactions sur plusieurs plateformes mobiles ainsi qu'auprès de divers appareils connectés afin d'assurer une expérience d'utilisation continue, principalement au niveau session. Par exemple, le concerteur permet de commencer un film sur la télé du salon, puis de prendre le transport en commun et d'en continuer le visionnement sur notre appareil mobile au gymnase.

2.4 Cadres applicables

Cette section présente divers cadre applicables aux activités de GIDIM. Or, certains de ceux-ci ne seront pas explorés en profondeur puisque leur étude pourrait faire l'objet d'une monographie à ce seul effet, et dépasse largement la portée de la présente étude.

2.4.1 Cadre normatif relatif aux données d'identité – discussion générale

Il existe nombre d'éléments qui permettent de cadrer les données d'identités d'un point de vue normatif et chacun de ceux-ci a un rôle particulier à jouer ainsi qu'une sphère où son influence est maximale. Il y a également une hiérarchie des éléments normatifs (Shelton, 2006) [166] et des *locii* d'impact différents. La présente section recoupe des réflexions et les centre autour des travaux de Eisenberg (1989)[167], Orlikowski (1992)[168] et plus tard de Venkatesh, JYL Thong et X Xu (2012)[169].

Le développement du cadre normatif pour la GIDI, le même que pour la GIDIM, se fait par sédimentation de l'évolution technosociale, comme c'est le cas pour nombre d'innovations, notamment celles adoptées par d'importants groupes sociaux ou ayant des impacts importants sur celles-ci. Suivent donc les phases qui ont été recensées comme jalonnant le développement de la GIDIM et leurs descriptions respectives.

D'abord, en matière de GIDI ou de GIDIM, comme pour tout développement scientifique ou technologique, il y a le fait. Ce fait est d'abord créatif, innovant et expérimental, voire

accidentel. À ce stade, il n'y a pas vraiment d'éléments normatifs. Le seul élément qui peut être considéré comme normatif peut être le caractère secret du partage de cette innovation. Cette phase s'appellera la phase 0.

Ensuite, il y a l'étude organisée de ce fait et de la théorie qui l'entoure. Cette « étude organisée » peut prendre plusieurs formes, dont l'exploitation académique (exploration scientifique) ou l'exploitation commerciale (et les phases de son adoption, par Xu, 2012), ou un mélange des deux. Peu après débute une étape qui connaît plusieurs cycles de développement concomitant à l'exploitation, soit celle de la rétroaction de la communauté (« *community feedback* ») qui l'adopte. Dans le cadre scientifique, il peut s'agir de revues de la littérature; dans le cadre commercial, il peut s'agir d'évaluation (« *reviews* ») des utilisateurs ou bien de versions par les fans « *fandrive* » ou « *homebrews* ». Souvent, c'est à ce moment que, lorsque cette réalité est imposée, elle peut connaître la plus vive résistance. Dans le début de cette phase, on constate usuellement le développement de normes techniques qui servent à organiser le développement et qui créent, ce faisant, des dynamiques de pouvoir entre les entités qui développent cette technologie. Dans le cadre commercial, c'est souvent là qu'Eisenberg constate qu'entre en ligne une sorte de paradoxe, voire une contradiction, où ceux qui promeuvent la technologie tentent de faire à la fois deux choses difficilement conciliables : ouvrir et fermer. Ainsi, ils tentent d'inciter le plus possible l'adoption de leur technologie (ouverture), mais ils essaient d'en préserver le contrôle (fermer), que ce soit par des brevets, d'autres formes de propriété intellectuelle, des éléments contractuels ou des situations de fait tels le monopole, l'oligopole ou le développement du militantisme (par exemple, le « cryptoanarchisme »).

Puis, les enjeux que suscite cette technologie viendront être encadrés par du droit spécifique du fait qu'ils deviendront importants pour la société et que les enjeux des utilisateurs deviendront les enjeux des citoyens. À ce deuxième stade, il y aura des lois spécifiques à cette technologie, du lobbying, des enjeux financiers importants.

Enfin, dans certains cas, les innovations sont parfois si importantes qu'il y aura des tractations politiques entre les nations à leur sujet. À ce troisième stade, il y aura des accords économiques et commerciaux, des traités politiques (ex : le nucléaire), des organisations

surpa-nationales qui seront promues afin qu'elles coordonnent cette technologie ou bien qui seront carrément créées à cette fin.

La GIDI semble traverser ces phases et être rendue à la phase II (codification en droit commun). Certains signes commencent à poindre relativement à la phase III (élaboration du droit international public), mais cela demeure encore prématuré (de conclure).

À la phase I (normalisation), il y a divers éléments normatifs qui ont façonné les aspects techniques de la GIDI. Que ce soit les normes Open ID [170 et 171] ou *OAuth* (IETF RFC 5849, puis 6749) [172 et 173] qui codifient les interactions sur le plan technique, ou bien les normes ISO/IEC 24760 qui dictent les aspects organisationnels en lien avec la GIDI, il existe diverses initiatives pour encadrer cette activité par des normes et des jeux politiques en lien avec cet encadrement. Il faut noter que cet enjeu a été si important que, malgré des positions de monopoles de fait importants, les normes applicables sont demeurées ouvertes et ce domaine n'est pas tombé captif des précarrés des principaux acteurs privés ou publics.

En ce qui concerne les données de la GIDI, celles-ci sont organisées, du moins à certaines étapes, sous des formes ouvertes, ce que les utilisateurs pourraient considérer fort heureux. Notons cependant que ces données représentées sous de telles formes ne sont que très parcellaires.

2.4.2 Législation applicable aux données d'identité

D'abord, les législations des divers pays encadrent plusieurs aspects de l'utilisation des données et parfois même la GIDI [173 à 181], incluant la GIDIM. Or, au Canada, contrairement à d'autres pays, il n'y a pas de loi qui gère à GIDI. Il y a cependant des lois connexes qui règlementent divers aspects de l'utilisation de technologies, tant au provincial qu'au fédéral et d'autres provisions de la loi couvrant des droits généraux s'étendent aussi dans le domaine de leur matérialisation et leur exercice dans un cadre électronique. Le concept juridique le plus proche de la GIDI(M) est la donnée nominative et l'élément législatif se rapprochant le plus d'une loi portant sur la GIDIM est la Loi concernant le cadre juridique

des technologies de l'information [182], et peu derrière suivrait la Loi sur la protection renseignements personnels (Canada) [183] et la Loi sur la protection des renseignements personnels dans le secteur privé (Québec) [185]. Notons que les lois fédérales protègent généralement l'individu contre l'État (droit public), peu importe le niveau ou palier et les lois provinciales dont le Code civil du Québec [184] couvrent la sphère entre individus privés ou entre individus et corporations privées, etc. L'étude de l'interaction entre les lois et les technologies saurait occuper une chaire de recherche pendant des années [187]. Alors, l'étude, même brève et seulement focalisée sur les contraintes de génie logiciel qui peuvent se dégager des lois pertinentes et de leurs impacts sur le domaine de la GIDIM, demeure toutefois un champ vaste et fertile; il serait très aisé de déborder amplement du cadre et de la portée fixés pour la présente étude. Il sera donc nécessaire d'adopter exclusivement l'angle très spécifique portant sur l'analyse des besoins des utilisateurs. À ce chapitre, les lois sont des mines de renseignements sur divers types d'utilisateurs ou cas d'utilisation prévus ou identifiés, ainsi qu'en matière des risques que le législateur cherche à mitiger à travers celle-ci. Enfin, notons une tendance assez récente et qui a marqué un cap au Canada, donc aussi au Québec, il y a quelques jours à peine : celle à l'effet que les États se rendent compte qu'ils sont dépassés par le caractère extraterritorial de la réalité numérique et que les tribunaux s'aventurent dans une avenue potentiellement risquée, surtout au chapitre des conflits d'obligations, sur le sujet de l'extraterritorialité des lois. En effet, l'arrêt Google Inc. c. Equustek Solutions Inc. (2017 CSC 34, CanLII) [186] confirme l'affirmation visée par le plus haut tribunal au Canada de la compétence extraterritoriale des lois et des tribunaux du Canada sur Internet.

2.4.3 Normes et autres cadres normatifs supplémentaires à la législation

Outre les contraintes juridiques et législatives, il y a d'autres considérations qui peuvent affecter la GIDIM. Il s'agit principalement des contraintes d'ordre pratique (autour de l'ergonomie), d'ordre parajuridique (extraterritorialité du droit et ses conflits) ainsi que techniques (normes de compatibilité technique). Enfin, viennent les bonnes pratiques en matière de GIDIM.

2.4.4 Contexte contractuel

Le cadre contractuel à l'étude est celui imposé par les opérateurs de plateforme, tant aux UFs, qu'aux développeurs d'applications et/ou fournisseurs de services (ci-après, opérateurs d'applications et/ou de services, « OAS ») et, dans le cas d'*Android*, aux fabricants de matériel. Ces extensions sont nécessaires, puisque ceux-ci pourraient, par ces contrats, se voir contraints, ou du moins influencés, dans leurs comportements envers les UFs, leurs décisions de conception ou bien leurs choix en matière de GIDIM. Au total, ce sont donc cinq (5) groupes de documents qui seront étudiés dans cette section : ceux applicables aux utilisateurs finaux d'*Android*, ceux applicables aux utilisateurs finaux de *iOS*, ceux applicables aux développeurs de logiciels sur l'*AppStore* d'*Apple* et ceux applicables aux développeurs pour Google PlayStore et, enfin, les « *Mobile Application Distribution Agreement* » ci-après « MADAs », applicables aux fabricants d'appareils fonctionnant sous *Android* lors de la vente.

Même si l'horizon est limité à ce nombre très restreint de quelques groupes de contraintes, la quantité de documents à analyser sera incroyablement grande. Cela est notamment dû à l'approche retenue, dans la rédaction de clauses, d'utiliser des inclusions référentielles. Cette technique s'apparente en philosophie et matériellement à la capacité de référencement par lien hypertexte à la base du HTML. Ainsi, un contrat peur référer à un autre contrat, qui à son tour peut référer à une panoplie d'autres documents et il y a donc une arborescence d'artéfacts à analyser. Par exemple, l'énoncé des termes de service de Google pointe à la politique de protection de la vie privée selon Google, laquelle pointe à son tour sur d'autres documents contractuels. Considérant que le premier document a force légale et qu'il subordonne le choix de cliquer « j'accepte » au fait d'avoir lu et d'accepter également les autres référencés, un utilisateur désirant être totalement conforme à ses obligations devra aller au bout de cette séquence documentaire, ce qui requiert un effort considérable, possiblement déraisonnable.

Du côté d'*Apple*, la licence applicable aux appareils *iOS* 10 fait 406 pages en petits caractères et porte de nombreuses références vers des documents externes. À cette réalité, il faut cependant apporter certaines précisions : cela inclut les versions en chaque langue pour chaque juridiction. La version « Français, Canada » fait 12 pages. Les autres artéfacts

auxquels il fait référence sont la politique des ventes [188] , le programme pour développeur d'applications [189], la politique de protection de la vie prive [190 et 191] , les conditions de *iCloud* [192], des références aux licences applicables des composants MPEG [193] et, étonnamment, pour la navigation sécurisée de Google, leurs Conditions d'utilisation [194] et Règles de confidentialité [195]. À leur tour, ces documents comportent des hyperliens. Par exemple, la page relative à la confidentialité fait quelques pages en impression et porte les liens vers quatre éléments : « Notre approche de la confidentialité » [196], « Gestion de votre confidentialité » [197], « Demandes d'info du gouvernement » [198] et « Politique de confidentialité », à proprement parler [199] . Ce dernier lien compte une vingtaine de liens hypertexte à son tour, dont les plus pertinents dans le contexte de la présente étude sont ceux qui font référence aux identifiants *Apple*ID ainsi que ceux faisant référence à la propriété intellectuelle. Notons également qu'une étude approfondie des termes et conditions [200] d'*Apple* permet de se rendre compte que des clauses importantes relativement à une matière (ex : vie privée) peuvent se trouver dans un endroit où on le suspecte le moins (« propriété intellectuelle ») ou externe (clauses relatives à la licence MPEG). L'obligation voulant que les contrats soient compréhensibles pour les consommateurs n'est pas nouvelle. L'idée était déjà recensée et étudiée en 1940 par Stuart Chase, dans son ouvrage « *The Power of Words* ») [201]. De nos jours, les phrases individuelles peuvent être claires, mais la compréhension de la somme de toutes les clauses, dans leur intégralité et la prise de conscience de ses effets, requiert un effort considérable. Cela pose des difficultés, d'une part, aux consommateurs qui adhèrent au contrat, lequel est un contrat d'adhésion, puisqu'il n'y a pas de négociation [208 et 209]. Cela pose aussi des difficultés aux décideurs, tels les juges, qui doivent statuer et allouer des ressources pour comprendre ces contrats avant de trancher. Devant une complexité croissante des documents ayant force contractuelle, dont ceux portant sur les termes et conditions, plusieurs approches peuvent être prises par les États qui assurent l'application judiciaire de ces obligations, chacune ayant ses avantages et inconvénients :

1) laissez-faire

2) invalider sans préavis les contrats qui seraient trop exigeants cognitivement (avec une approche judiciaire à la 159191 Canada inc. (Discount Location d'autos et camions) c. Waddell [202 et 203] ou Dell Computer Corp. c. Union des consommateurs, [2007] 2 .C.R. 801 [204], ou bien avec une approche à la « *Minnesota Plain Language Contract Act* »)

3) imposer des obligations modérées capables de circonscrire la charge cognitive sous peine de rendre le contrat nul

4) Imposer des obligations très douces sur la clarté des contrats (*New York Plain English Law, N.Y. Gen. Oblig. § 5-702)* [206 et 207]

5) introduire des automates dans le processus, au risque de rendre l'analyse impraticable « à la main », par des humains

Au sujet de cette dernière option, le concept « d'assistant virtuel » répond. Si les obligations contractuelles étaient modélisées formellement, cela évacuerait tout besoin d'interprétation et des machines pourraient aisément traverser ces volumes importants de données et extraire des conclusions normalisées et communes. Bref, les arbitres, puis les tribunaux automatisés glisseraient le pied dans la porte. Si les priorités des clients, de plus en plus exigeants et sensibles, étaient également modélisées formellement, il pourrait y avoir des analyses automatisées qui pourraient avoir lieu afin d'établir des opinions normalisées de congruence ou de divergence; bref, si le système recommande de signer ou pas. Il pourrait même y avoir des négociations automatisées avec des critères pondérés. Le danger dans tout cela est que l'on confie à des automates la gestion de la raison juridique, un domaine où ils sont certes plus performants que nous, mais qui a également comme particularité de guider nos vies et d'organiser nos sociétés modernes. Dans le même ordre d'idées, certaines protections sociales seraient probablement abandonnées. Par exemple, si les contrats sont négociés, les protections propres aux contrats d'adhésion ne tiennent plus. Il faut aussi garder à l'esprit qu'il y a un risque d'aggravation de l'asymétrie de droits découlant de l'asymétrie de moyens. Notons enfin que, dans la situation actuelle, il existe déjà un début de telle situation et il s'agit de technologies de type « *Privacy Guard* » sous Google *Android* ou, plus simplement, des plus dernières interfaces d'installation d'applications sur mobiles. Ces assistants se limitent, cependant, aux demandes de permissions déclarées au niveau « application » dans une étape préalable à l'installation de l'application. Ainsi, l'interface informe l'utilisateur que l'application qu'il désire installer demande, par exemple, l'accès au micro et aux fichiers. Si on analyse le cadre juridique actuel, mais également la politique libérale qui anime les grands traités commerciaux auxquels nos nations adhèrent depuis quelques années, les options 2 et 3 ne peuvent demeurer sur la table. L'option 1, identifiée plus haut, n'est pas en soi une option de changement et l'option 4 peut être perçue comme évidée de toute capacité de contrainte. Restent donc les options, aux antipodes, 1 et 5, le *statu quo* ou les automates. Ayant d'abord

abordé la difficulté cognitive imposée par la lecture des contrats liant l'utilisation des plateformes et applications mobiles, vient ensuite l'étude de la fréquence de lecture de ces termes et conditions. Les travaux de Bakos et Marotta-Wurgler (2014) [210] sont compatibles avec les données recueillies dans des versions précédentes du présent mémoire, lesquelles permettent d'estimer qu'environ 0,11 % des utilisateurs (environ 1 sur 1000) lisent les termes et conditions, et cela dans le cas de comptage le plus généreux, où on se réfère uniquement à la lecture du principal élément contractuel. S'il fallait, pour satisfaire le critère de lecture, avoir lu tous les éléments constituant l'intégralité du contrat, ces chiffres seraient encore plus bas. Ce constat sera repris aux résultats.

À ce stade, il faut se demander pourquoi il est important de mettre l'emphase sur le fait que les termes et conditions soient difficiles à lire, mais aussi sur le fait qu'ils ne soient pas souvent lus. L'idée derrière ces emphases est de faire ressortir les conclusions confirmées par les travaux de Cotton et Bloan (2011) [211] sur les perceptions des utilisateurs quant aux contrats dans les environnements mobiles et représentant un cas spécifique des réflexions de Ben-Shahar (2009-20114) [212, 213 et 214]. En l'espèce, les utilisateurs considèrent que les termes sont trop longs, qu'ils ne peuvent rien y changer, qu'ils n'envisagent pas d'exercer leurs droits de toutes manières et qu'ils sont, somme toute, assez similaires. Par ailleurs, dans les travaux de Cotton et Bloan, il y a déjà des marqueurs qui pointent vers d'autres réflexions, notamment le fait que plusieurs utilisateurs estiment qu'ils ne peuvent pas être assujettis à ces termes semble pointer vers le fait qu'il y ait des stratégies de mitigation (ex : utilisation de fausses identités ou de la pseudonymie) qui soient adoptées par ceux-ci. De tout cela se dégage un état d'esprit à l'effet que l'utilisateur est contraint de céder ses droits et prérogatives, de manière inconditionnelle; une telle situation en étant une de non-droit. Devant une telle situation, le remède traditionnel est l'ordre public de protection. Or, ce genre de mesures est incompatible avec la philosophie libérale des gouvernements actuels. De plus, il faudrait qu'il y ait un mouvement plus étendu puisque, si une seule juridiction légifère en ce sens, il est plus facile et attrayant pour l'opérateur de perdre formellement ce marché (laissant donc le tout au marché noir ou indirect) à la concurrence que de créer une brèche au front juridique qu'elle essaie de dresser autour de ses droits et prérogatives. Sur ce dernier point, notons avec une certaine fierté que, lors du lancement du *XCode Studio* et du programme pour développeurs d'applications, *Apple* semblait considérer que le Québec (dont Montréal) constituaient une population

suffisamment prioritaire en termes de créateurs, programmeurs et entreprises de développement informatique qu'elle a consenti à quelques pirouettes afin de ne pas se priver de ce marché, notamment en baissant l'échine devant la Loi 101 [215].

Ayant établi que le contexte n'est pas favorable à des rapports équitables entre les utilisateurs et les opérateurs, il est maintenant à propos de se pencher sur certains éléments de ce corpus contractuel afin de le comparer avec les besoins des utilisateurs en matière de GIDIM. Ainsi, en Annexe B seront présentés quelques extraits des soixante-et-un (61) document légaux [200] auxquels sont astreint les utilisateurs du *iPhone* version *iOS* 10, ainsi que la quantité un peu plus grande de documents régissant les développeurs d'applications pour cette plateforme. Ensuite, l'Annexe C comporte l'équivalent du côté de Google. Les discussions et analyses de ces extraits sont donc résumées dans le reste de la présente section.

D'abord, il faut constater une chose : ces amas de clauses se distinguent, outre que par leur volume et leur complexité déjà mis en emphase, par la prouesse avec laquelle ils cherchent à concilier une défense des droits des OPs tout en tentant de préserver une image favorable, voire de défenseurs des libertés individuelles. Ensuite, il faut constater que, du moins sur la forme, il y a une différence importante entre l'approche de Google et celle d'*Apple*, la première affirmant explicitement qu'elle tient à ce que les données des UFs demeurent la propriété exclusive de ceux-ci. Certes, il y a dans les deux cas des licences très larges qui sont accordées aux opérateurs, mais Google se distingue par cette déclaration explicite.

Ensuite, si on analyse à la loupe, les clauses en aux Appendices A et B, on se rend compte que dans les deux cas, les conclusions essentielles suivantes se dégagent :

1) Il y a une licence très large accordée aux opérateurs de plateforme.
2) Toutes sortes de données sont collectées automatiquement par les appareils ou les services dont les données de localisation. Le seul moyen de désactiver la collecte de ces données par les opérateurs est de désactiver les services (certains doutent même que ces données cessent d'être recueillies lorsque l'on désactive le service).
3) Il y a une stratégie très agressive de déclinaison de toute responsabilité de par les OPs.
4) Il y a des pratiques très opaques de rétention des données.

5) Les données recueillies ne sont cryptées que d'une manière accessible aux OPs.

6) Les données recueillies peuvent être partagées avec les autorités étatiques.

7). Les services et les conditions d'utilisation peuvent être modifiés à tout moment par l'OP.

8) En cas de désaccord avec les conditions, la seule option est d'arrêter d'utiliser les produits

Ces observations seront intégrées aux résultats.

Ensuite, en ce qui concerne les conditions auxquelles sont astreintes les développeurs de contenu, du côté d'*Apple*, celles-ci ne peuvent pas être légalement reproduites puisque, avant même de pouvoir avoir accès à ces conditions, il faut accepter d'être lié par des conditions préliminaires qui empêchent même la diffusion, par clause de non-divulgation/ confidentialité, des clauses et termes supplémentaires auxquels les développeurs sont assujettis. Similairement, les ententes MADAs [216 à 223] sont également confidentielles du côté de Google. Il existe cependant des fuites et des sources officieuses qui permettent d'accéder à des versions de telles ententes [219 à 222].

Ainsi, en voici les éléments saillants dans le cadre de la présente étude :

1) Du côté des MADAs de Google, les droits des UFs ne semblent pas davantage compromis. Il n'y a pas de directives, du moins pas dans ce qui a été recensé et est présumé être une version authentique d'une entente MADA, d'instructions visant à forcer le constructeur à ajouter davantage d'éléments de capture de données ou des éléments à l'insu de l'utilisateur. Il n'y a pas non plus d'éléments de marquage ou de métadonnées outre ceux publiquement connus. Cependant, il y a : un important resserrement de manière à décourager les utilisateurs d'adopter des plateformes alternatives; des éléments de normalisation de l'expérience Google et de placement de produits Google, lesquels semblent surtout vouées à donner un avantage concurrentiel à Google afin de préserver l'état de fait où une grande majorité des utilisateurs sous *Android* le sont sous une version menée et opérée par Google plutôt qu'une mod; et, une autre exception recensée, qui fait un peu sourciller côté sécurité, est le fait que le contenu web doive forcément être rendu par un moteur de rendu Google.

2) Du côté d'*Apple*, les clauses imposées aux développeurs limitent grandement leurs options de développement, assujettissent la conception de logiciels à l'approbation finale et assez arbitraire d'*Apple* et exigent notamment l'utilisation de services et composants programmatiques fournis par le système plutôt que développés par les développeurs. Par exemple, en matière de cryptographie, ce sont les librairies du fabriquant qui doivent être utilisées et non des librairies de tiers ou développées par le développeur de l'application. On peut comprendre que cela puisse émaner d'une bonne intention visant à éviter que de mauvaises mises en œuvre soient employées, mais ultimement, cela se fait au détriment de la diversité des options et rend le tout tributaire de la qualité et des fonctionnalités de la librairie fournie par le système et de la confiance qu'elle peut mériter.

Du côté d'*Android*, les conditions imposées aux développeurs d'application sont publiques et semblent mettre de l'avant le fait que Google ne désire pas jouer un rôle aussi centralisateur qu'*Apple* et que, en conséquence, son approche est minimaliste. Les principales observations sont, encore une fois, relatives au fait que Google semble vouloir éviter de se faire déborder par le côté par des versions alternatives.

2.4.5 Jurisprudence

Encore une fois, il ne sera pas ici l'occasion d'analyser les tendances jurisprudentielles en matière de renseignements personnels, ni de GIDI, ni même de GIDIM. L'idée de brosser un tableau général de la jurisprudence est simplement de permettre de comprendre qu'il existe bel et bien des contrepoids constitutionnels à l'action de l'exécutif en matière d'interférence sur les communications et appareils mobiles, mais que ces protections méritent d'être démystifiées et précisées. Leur portée et leur teneur peuvent être surestimées dans le discours ou l'inconscient populaire et cela mérite clarification par l'épreuve des faits. L'essentiel à retenir se résume en deux tableaux (qui sont dans la section [S: 4.1.3]). Le premier illustre le fait que les tribunaux entrent de plus en plus en contact avec les réalités propres au monde virtuel et à l'utilisation des TIC, notamment en puisant de la preuve dans les données de GIDIM, celles-ci étant devenues des sources de prédilection à cet effet. Le deuxième tableau illustre la facilité avec laquelle il est possible pour l'exécutif de l'État (police) d'obtenir une autorisation judiciaire pour intervenir dans les communications privées; bref, d'utiliser les

données de GIDIM contre le gré ou à l'insu des UFs, mais surtout qu'aucun cas n'est refusé pendant la période pour laquelle les données sont disponibles.

Du corpus jurisprudentiel étudié, les quatre autres décisions sélectionnées comme les plus pertinentes à l'égard de la présente étude sont Mahjoub (Re), 2014 CF 479 (CanLII) [224], R. c. Spencer et R. c. Vu [226] et R. c. Fearon [227] Dans l'affaire Mahjoub, la Cour (fédérale) reconnaît l'importance du droit d'accéder à divers services en ligne pour les individus et, même dans le cas d'un individu visé par un certificat de sécurité, la Cour a choisi de permettre à l'individu d'avoir accès à Internet, à condition qu'il n'utilise aucun moyen d'entrave à l'analyse judiciaire (« criminalistique informatique ») du contenu de son ordinateur, ni de son portable, et qu'au besoin, il divulgue tous ses mots de passe à l'Agence des Services Frontaliers du Canada (ASFC). Dans le cas de Spencer, la Cour Suprême du Canada établit que la communication de (méta-)données relatives aux télécommunications (incluant les données de GIDIM et de positionnement, de par leur description, sans toutefois les nommer ainsi), par les opérateurs d'infrastructure à des tiers, requiert l'obtention préalable d'une autorisation judiciaire. Dans Vu, la Cour Suprême du Canada établit que la fouille de données sur un ordinateur et sur un cellulaire nécessitent un mandat et doivent se conformer aux limites de celui-ci. Toujours dans le cas de Vu, le but était justement d'établir plusieurs faits dont l'identité des opérateurs d'une plantation clandestine de cannabis.

Enfin, dans le cas de Fearon, la Cour conclut que la fouille d'un appareil cellulaire, que celui-ci soit protégé par un quelconque mécanisme, est permise à l'intérieur de certains paramètres, sans toutefois obliger le suspect à apporter quelque collaboration que ce soit. Les paramètres à l'intérieur desquels cette fouille peut être valide sont essentiellement que l'arrestation soit légale, que la fouille soit accessoire à l'arrestation et raisonnable, qu'elle se déroule sur place et soit limitée aux moyens immédiats des policiers, puis, que la fouille soit dirigée (dans but précis) et adéquatement documentée. Cela constitue un recul important compte tenu de la tendance inscrite par les deux décisions précédentes, mais demeure quand-même une décision respectueuse de l'auto-détermination des utilisateurs en matière de GIDIM si on la compare à la décision américaine *Virginia v. Baust, No. (CR14-1439; Va. Cir. Oct. 28, 2014)* [228] prise à environ la même époque et analysée dans l'article « *Court Rules Police May Compel Suspects to Unlock Fingerprint-Protected Smartphones* » (2014) [229] du « *JOLT*

Digest » (« *Harvard Journal of Law and Technology* »), par les auteurs Ken Winterbottom (en rédaction) et Yixuan Long (en édition et mise à jour).

À la lumière de ces cas cités et étudiés, on peut conclure que les protections constitutionnelles, tant au Canada qu'aux États-Unis ne sont pas absolues, qu'elles tendent même à s'amenuiser dans le cadre de leur récente évolution, notamment sur les plateformes mobiles si on suit les cas/jurisprudences Fearon et Baust.

2.5 Considérations d'affaires

L'évolution des méthodes de GIDIM sont affectées par diverses considérations dont celles liées aux perspectives d'affaires. Pour ce motif, il est pertinent d'exposer les principaux modèles d'affaires identifiés ainsi que comment les entreprises créent de la richesse à partir des données ou y aspirent.

2.5.1 Modèles d'affaires

La présente section présente divers modèles d'affaires tels que décrits dans la littérature étendue (pas uniquement académique). Il est à noter que la plupart des articles scientifiques revus par les pairs portant sur les modèles d'affaires ont des dates de parution se concentrant entre 2001 et 2007. De ce fait, ils ont plus de dix ans et ils précèdent nombre de changements qui se sont opérés pendant le dernier tiers de la période couverte par la présente étude. Un effort supplémentaire a donc été investi afin de trouver au moins trois études pertinentes plus récentes (au-delà de 2007) en la matière.

Un des études les plus récentes de la littérature et retenue dans le cadre de la présente recherche s'intitule « *Business Model Innovation through Trial-and-Error Learning – The Naturhouse Case* » [230]. Elle illustre l'importance de la nécessité de faire évoluer les modèles d'affaires et étaye les principaux facteurs de résistance à cet égard. Il s'agit cependant d'une étude de cas et elle n'est pas spécialisée au domaine de l'informatique et encore moins de celui de la GIDIM. Il n'en demeure pas moins que cela illustre des préoccupations

récurrentes relatives aux modèles d'affaires. La plus récente (macro-)étude retenue sur le sujet (« *The Business Model: Recent Developments and Future Research* ») [231] va dans le même sens et constate que cet aspect gagne en importance.

> *« From the point of view of the focal firm, the activities of external innovators can be organized as a collaborative community or as a market (Boudreau & Lakhani, 2009), which in turn implies different business model configurations: in the former (community), members are often willing to collaborate and work for free, while in the latter (market) innovators develop multiple competing varieties of complementary goods, components, or services, with little cooperation among them.*
>
> *There is an increasing consensus that business model innovation is key to firm performance. A significant number of scholars focus on business model innovation as a vehicle for corporate transformation and renewal (e.g., Demil & Lecocq, 2010; IBM Global Business Services, 2006; Ireland, Hitt, Camp, & Sexton 2001; Johnson, Christensen, & Kagermann, 2008; Sosna, Trevinyo-Rodríguez, & Velamuri, 2010). Bouchikhi and Kimberly (2003) and Chesbrough (2010) have identified barriers to business model innovation in existing firms, such as the configurations of assets and processes, which may be subject to inertia, as well as the cognitive inability of managers to understand the value potential of a new business model. »*

En fait, les documents académiques les plus pertinents quant à l'utilisation de modèles d'affaires dans le cadre de la présente étude sont les suivants : « *A Privacy-Enhancing e-Business Model Based on Infomediaries* » (2001) [232] , « *E-Business Model Design, Classification, and Measure-ments* » (2002) [223], « *The business Model Ontology – A proposition in a design science approach* » (2004) [234], « *The utility business model and the future of computing services* » (2004) [235], « *What Is Web 2.0: Design Patterns and Business Models for the Next Generation of Software* » (2005) [236] et « *The Business Model: Recent Developments and Future Research* » (2011). Les documents dont la publication remonte avant 2007 tendent à favoriser l'évolution des modèles d'affaires (relatifs aux données) qui s'alignent sur le modèle des services publics (« *utilities* », tels l'eau et l'électricité). Ceux rédigés après cette date semblent prendre note de la valeur croissante qui est accordée aux connaissances tirées des données comme matière première et du fait que

cette valeur ajoutée peut être supérieure à celle provenant des aspects « utilitaires » du modèle d'affaires.

Ensuite, dans « *The business Model Ontology* (…) » et « *E-Business Model Design, Classification, and Measurements* » Osterwalder et al. y mettent en garde le chercheur contre la tentation de rapiécer des modèles d'affaires nouveaux à partir de modèles précédents. Ceux-ci appartiennent à des familles et des classements différents, le plus souvent cela est dû au fait que des éléments opérationnels sont très distincts ainsi qu'à des divergences de culture qui se reflètent tant dans les objectifs d'affaires que dans divers aspects opérationnels et relationnels avec le public-cible.

À la lumière de ces enseignements, les sous-sections suivantes illustreront simplement des modèles d'affaires et les évalueront quant au rôle qui y est réservé à la GIDIM.

Bien connaître les modèles d'affaires est essentiel pour les développer et cela est nécessaire à faire évoluer le domaine. Dans tout système économique, une activité souhaitable doit trouver comment se financer et assurer sa pérennité. De plus, dans le cadre d'une économie capitaliste qui est la nôtre, toute activité doit pouvoir présenter un potentiel de dégager un profit et cela doit se faire de manière décomplexée. Culturellement, il faut accepter qu'il est nécessaire de reconnaître le caractère sain d'un profit raisonnable dans l'élaboration de modèles d'affaires vers lesquels ont désire faire évoluer l'économie et, si l'on cherche à développer un capitalisme plus vertueux, plus respectueux des droits individuels et des valeurs collectives, il faut faire preuve de créativité et aligner les incitatifs de manière à ce que cette vertu soit récompensée et puisse être perçue comme attrayante sur plusieurs aspects dont celui financier.

Modèle basé sur la vente d'appareils [237 et 238]

Ce modèle se base sur la capacité de convaincre l'utilisateur d'acheter un produit à forte valeur ajoutée que le marchand produit. Les avantages perçus par l'utilisateur doivent impérativement provenir de l'achat de l'appareil. La profitabilité du modèle provient de la capacité à rendre l'objet attrayant, à en réduire le coût de production et d'opération ainsi qu'à

en augmenter l'adoption. Les coûts peuvent être incompressibles puisqu'il s'agit d'un objet réel. Il est donc important de favoriser la mise en valeur du bien et de ses accessoires. Cela peut se faire notamment par le développement d'une communauté et d'une image de marque. En matière de GIDIM, l'utilisateur est géré et cela peut se traduire par la tendance de l'opérateur de la plateforme à le prendre en charge et à veiller (peut-être de manière trop zélée) à mieux le connaître pour mieux le servir et à tout faire pour le garder dans son giron, tout en favorisant le rachat continuel d'équipement plus moderne, quitte à parfois faire dans l'obsolescence programmée.

Modèle basé sur la vente de licences individuelles [239, 240 et 241]

Ce modèle se base sur la capacité de convaincre l'utilisateur de dépenser pour acheter des licences d'un produit logiciel ou du contenu. Tout d'abord, l'idée de devoir payer pour un objet intangible à coût nul connaît une certaine résistance inhérente à divers *a priori* des mentalités dans nombre de cultures, notamment au chapitre de l'équité. De plus, ce modèle exige que les licences soient individuelles et ne puissent pas être transférées, ce qui peut accroître ce sentiment. Ce modèle est commun à *Apple* et à Google, quoique chez *Apple* cette mentalité soit philosophiquement plus proche.

En matière de GIDIM, l'opérateur doit principalement s'assurer que les normes d'attribution des accès et licences sont sévèrement appliquées. Pour ce faire, il peut être intéressé par le déploiement d'un environnement doté de mesures permettant de contrôler de manière détaillée l'identité des individus. Notons que cette approche a quelques similarités à celle de vente d'appareils, à l'exception qu'une fois le coût de développement amorti, le coût de production par copie du logiciel/contenu est presque nul.

Modèle basé sur la vente de publicité (affichage) [242 à 249]

Ce modèle se base sur la capacité de convaincre d'une part des utilisateurs de recevoir du contenu et, d'autre part, de convaincre des annonceurs de payer pour diffuser leur contenu. Dans ce modèle, le payeur est l'annonceur et, en quelque sorte, l'utilisateur est la marchandise, du moins la promesse de la capacité d'accéder à son attention est ce qui est transigé. Ce modèle requiert le plus grand contrôle possible sur l'utilisateur puisque sa liberté

augmente le risque de l'opérateur de ce modèle. Au bout du compte, l'annonceur cherche à augmenter la probabilité que l'utilisateur décide de dépenser pour consommer un des produits de ce dernier et le montant dépensé en publicité doit être statistiquement inférieur au montant de gain probabiliste de déclenchement d'un achat menant au profit. En soi, ce parcours de génération de plus-value est parmi les plus complexe et il n'a des chances de réussite que dans la mesure où l'opérateur de la plateforme dispose d'une connaissance très intime de l'utilisateur et qu'il sait comment le « forcer » à procéder à un achat. Pour y arriver, l'opérateur doit canaliser, voire susciter le désir de procéder à l'achat. Attendu que les chances de réussite sont inhéremment faibles, l'opérateur doit pouvoir disposer d'un maximum d'informations pour tenter de mieux associer des annonces à des individus, de manière à ce que l'exposition soit la plus susceptible de réussir. Cette opposition intrinsèque entre les intérêts des utilisateurs et ceux de l'opérateur peuvent expliquer la genèse de nombre de problèmes mentionnés dans la présente étude puisqu'un comportement prévisible et contrôlable réduit son risque.

Cette approche revêt également la particularité intéressante du point de vue scientifique provenant de la capacité offerte d'accéder aux outils analytiques offerts aux annonceurs. Ceux-ci permettent à tout chercheur de connaître ou de confirmer, du moins en partie, la nature des renseignements recueillis. Bref, si, en tant qu'utilisateur, on se sent dépouillé de ses informations, lorsque l'on se met dans la position de l'annonceur, on peut suivre la trace et constater comment nos données sont commercialisées et valorisées.

En matière de GIDIM, cette approche est celle qui semble le plus expliquer l'état actuel de la situation et la propension des opérateurs à vouloir intercepter chaque élément d'identité possible. De plus, ce modèle met de l'avant l'incompatibilité inhérente entre ce modèle et le fractionnement de l'identité puisque les acheteurs cherchent à obtenir un client et non pas un fragment de client.

Modèle basé sur la vente de publicité (recherches) [250 à 254]

L'approche basée sur la vente de publicité dans les recherches ressemble beaucoup à celle décrite plus haut, mais où les intérêts de l'utilisateur peuvent être conciliables et *a priori* le

sont avec ceux de l'opérateur. L'utilisateur cherche la meilleure information, la plus pertinente et le travail de l'opérateur permet de l'aider en ce sens. Cette aide n'est pas parfaite, ni parfaitement sincère, mais elle est quand-même considérable. De plus, l'utilisateur se doute bien du caractère imparfait de cette aide et décide, parmi les choix proposés, d'utiliser l'engin de recherche qui lui est le plus utile. C'est pour ce motif que divers engins de recherche qui ont su dépasser le seuil de tolérance de l'utilisateur et accorder une importance trop grande à la publicité ou ne pas fournir des recherches de qualité, ont perdu de l'utilisation. Ce n'est pas commun avec les engins de recherche généraux, mais c'est le cas fréquemment avec les engins de recherche spécialisés : fonction « recherche » dans les forums, les sites de vidéo, les sites de torrents, les sites de téléchargement de logiciels, etc.. L'équilibre efficacité vs. publicité constitue même un élément fondateur de la confiance que sollicite un site web et cela est davantage remarqué dans les sites web proposant du contenu exécutable à télécharger.

Dans ce modèle, l'opérateur influence les résultats de recherches de l'utilisateur afin de favoriser les résultats commandités. On retrouve l'opposition d'intérêts, mais sous une forme adoucie et moins apparente puisque l'opérateur n'a pas à susciter l'envie chez l'utilisateur, il n'a qu'à l'influencer et le diriger puisque celui-ci est déjà spontanément intéressé, c'est lui qui initie la recherche. En matière de GIDIM, la connaissance de l'utilisateur ne sert donc pas à générer une vente, mais à la canaliser ou à l'orienter. Cela se traduit par le fait qu'une recherche individuelle réalisée il y a quelques semaines puisse encore hanter l'utilisateur sous forme de personnalisations des résultats de recherche pendant une durée indéterminée.

Modèle basé sur les services [255 à 279]

Les modèles d'affaires basés sur les services se caractérisent par le fait que l'opérateur développe une compétence spécialisée et cherche à obtenir rémunération pour la fourniture de ce service. Outre le prix, c'est la qualité de ce service et sa réputation qui sont les principaux éléments pour convaincre l'utilisateur de retenir ce service. Il faut donc être le meilleur ou se voir perdre des parts de marché au profit de la concurrence. Là où cela devient un peu plus compliqué, c'est qu'il y a trois principaux modèles de financement et que le financement dicte les allégeances et les influences.

Le premier consiste en le financement direct par l'utilisateur. Dans ce mode, l'utilisateur est roi et l'influence de tiers est mineure, voire nulle. Un second mode est le financement par un tiers neutre et désintéressé (l'État, une fondation, un OSBL, etc.). Ce modèle peut être exemplarisé par un outil de recherche d'emploi offert par Emploi Québec ou bien Wikipédia. Notons cependant que rares sont les commanditaires qui ne cherchent aucunement à influencer l'utilisation. Un troisième mode est celui où le financement est pourvu par une tierce partie, laquelle dicte ses conditions. Dans ce troisième cas, la GIDIM sert notamment à assurer un rôle de ticket-modérateur et à assurer l'adéquation de l'utilisation de ressources de manière conforme au modèle de financement, bref à s'assurer que c'est bel et bien un utilisateur valide qui mobilise ou consomme des ressources et qu'il est/sera donc possible de (le/la) monétiser. De plus, il se peut que les impératifs ou intérêts du tiers qui finance dictent de colliger le plus d'information possible de la part de l'utilisateur, dans lequel cas, les fonctions de GIDIM servent également à la collecte de renseignements personnels à touts azimuts. Voici quelques exemples de services :

A) Identité en tant que service (« *Identity as a Service* »)

Le premier type de service, lequel devrait, à la lumière de son caractère fondamentalement sensible, offrir une allégeance indéfectible et exempte de toute influence extérieure, serait un modèle d'affaires basé sur les services d'identité. De tels services sont recensés dans la littérature. Outre l'individu et, éventuellement, l'autorité qui garantit l'identité, il ne devrait pas y avoir de tierce main. Cela ne signifie cependant pas que le fournisseur de service pourrait se prêter à accepter les requêtes douteuses de ses clients, telles la personnification d'autrui. Il y a des règles à respecter puisque ce genre de service, pour être utile, doit également être reconnu comme fiable par des tiers. Or, en matière de GIDI(M), sous ce modèle, c'est l'utilisateur qui décide du niveau d'exposition de son identité et des stratégies (d'unification, de composition, de transcendance, de morcèlement, d'obfuscation, etc.) y étant relatives. Ainsi, si un utilisateur préfère divulguer moins de détails, mais être contraint à être limité dans les fonctionnalités, c'est son choix libre et éclairé et le système doit lui permettre d'exercer ce choix et de moduler son niveau de protection de la vie privée.

B) Application en tant que service

Ce modèle d'affaires est adopté principalement par les opérateurs d'applications et vise à offrir divers services : agrégation de nouvelles, accès au contenu, stockage en nuage, capacités transactionnelles, capacités diverses et variées, etc. Dans ce modèle, il est possible de dégager des revenus accessoires (qui peuvent néanmoins être importants) à partir des données. Il se peut que divers impératifs éthiques commandent de ne pas sous-estimer les utilisateurs, ni leurs aspirations en matière de désir d'autodétermination quant à leurs données [279].

C) Infrastructure en tant que service

Un modèle qui est aussi vieux que la téléphonie mobile est celui de l'infrastructure en tant que service. De manière classique, il s'agit du modèle part lequel l'opérateur d'infrastructure (généralement de télécommunications) reçoit une compensation pour le service qui consiste en donner accès à son infrastructure, aux frais de l'utilisateur. Dans ce cas, la GIDIM peut principalement servir à rattacher une utilisation à un compte et à permettre le paiement, voire le recouvrement de ce compte en mode post-payé. En mode prépayé, soit l'utilisation est illimitée (ou s'y apparente), ou elle est limitée et inextensible, mais dans les deux cas, il ne peut y avoir de solde débiteur au bouf de l'exercice, ce qui permet notamment d'opérer de manière anonyme. Notons que parfois le réseau connaît des limites inférieures à la demande et qu'il est sain et nécessaire de limiter l'accès. Or, parfois, ces tickets-modérateurs ne servent qu'à maximiser les profits. La GIDIM permet également aux opérateurs de limiter leurs risques et, en cas d'utilisation problématique des infrastructures (ex : envoyer des pourriels ou des menaces de mort), elle facilite la traçabilité et l'imputabilité des utilisateurs.

Or, depuis que la neutralité des infrastructures est devenu un enjeu, principalement autour du débat de la « *neutralité du Net* », il est apparu clair que les opérateurs d'infrastructures sont susceptibles de tenter d'utiliser leur rôle essentiel dans cet écosystème pour influencer divers autres joueurs et, au bout du compte, gagner un avantage. Ces jeux d'influence vont de la limitation de la vitesse de connexion à l'effacement pur et simple des annonces. Divers opérateurs tant applicatifs que de plateforme ont donc décidé de faire des incursions dans le

domaine de la fourniture de services d'infrastructures pour pouvoir s'assurer que nul ne puisse se mettre à l'entrave de leurs précieux UFs. Diverses questions quant à l'intégration des modèles d'affaires sont alors soulevées. En matière de GIDIM, tant dans le modèle classique que dans le modèle incluant les nouveaux joueurs, les opérateurs d'infrastructures de télécommunications (OTs), sous la tendance actuelle des choses (sauf si l'usage de technologies comme Tor en venait à gagner en popularité) et puisqu'ils sont capables de connaître en détail ce qui circule par leur infrastructure, sont assis sur une mine de données. Par conséquent, ils peuvent être tentés justement d'y piocher et de convertir ce « *Big Data* » (« giga données ») en « *Big Money* » (gros sous, giga profits). Certains opérateurs étrangers (AT&T) vont même jusqu'à offrir au client deux choix : un accès rapide et plein prix, pour lequel les « préférences Internet » (« *Internet Preferences Program* ») ne sont pas scrutées et un service 29 U$ moins cher où l'utilisateur accepte de participer à ce programme d'analyse et étude des habitudes de navigation. Il est même possible d'obtenir un service « gratuit », où seul l'amortissement initial (de 300 U$) est défrayé, mais ensuite sans frais mensuels, à condition de faire partie de ce programme. Outre le fait que d'un point de vue technique, cela requiert de passer par des serveurs mandataires, ce qui n'est peut-être pas une bonne idée pour un bassin de population si grand et des contextes d'utilisation si variés, cela soulève également des questionnements majeurs en éthique et en sécurité.

D) Autres services

Il existe une panoplie d'autres modèles d'affaires basés sur les services, mais les méthodes de financement restent essentiellement les mêmes. Les plus intéressantes exceptions sont celles liées aux méthodes de paiement électroniques, que ce soit les monnaies cryptographiques ou bien les marchés automatisés, il y a peut-être des réponses pertinentes aux questions relatives au financement des services de ce côté.

Modèles basés sur la valeur des données

Il y a des modèles d'affaires plus obscurs et ceux-ci visent principalement la valeur des données. Il existe des modèles d'intermédiaire ou de courtage en ce domaine. Par exemple, *Whitepages* offre un service permettant d'avoir accès à des données personnelles sur des

individus. Or, pour obtenir le rapport, il faut fournir des données sur le demandeur et, ce faisant, celui-ci bonifie la base de données dont l'opérateur dispose pour effectuer son business. Il y a des modèles moins avouables qui tirent avantage de l'importance liée à la valeur des données et dont les abus peuvent prendre diverses formes. Un exemple qui a récemment fait le tour du monde et s'est même retrouvé relayé sur les pages du *Financial Times* [280] provient initialement d'un journal local de la province de Guangdong, le *Nandu Daily*. Bien que le modèle d'affaires soit sommaire et ne comporte pas tous les éléments nécessaires à son étude selon les méthodes reconnues par l'académie, il permet parfaitement d'illustrer l'idée qu'un modèle d'affaires, aussi primitif soit-il, peut se baser sur l'importance des données relatives à l'identité ainsi qu'à la réputation. En l'espèce, l'article du *Financial Times* rapportait que des prêteurs privés exigeaient comme collatéral, auprès de leurs jeunes emprunteurs de sexe féminin, de leur fournir des images de nudité exhibant leurs pièces d'identité, ces images étant prêtes, selon les termes de l'entente, à être divulguées au loisir du prêteur, en cas de défaut de paiement du principal et des intérêts élevés.

Un autre modèle d'affaires, plus sophistiqué et ayant un impact local est celui de Globe24h [281] (et accessoirement reputation.ca). Après avoir obtenu illégalement (de manière contraire aux conditions d'utilisation) le contenu de plusieurs dossiers judiciaires disponible à partir de CanLii (lequel est à son tour abreuvé par la SOQUIJ et le Ministère de la Justice pour ne nommer que ceux-ci), un entrepreneur roumain a mis sur pied un site qui, de par la manière dont il est conçu, met à contribution les capacités de Google, afin que lorsque quelqu'un y effectue une recherche portant sur le nom d'un individu, si cet individu se trouve dans les bases de données de l'entreprise, ce sont les détails judiciaires les plus embarrassants qui se retrouvent associés à son nom au haut de la liste des résultats. Pour pallier à cette situation, l'illustre entrepreneur propose de régler ce fâcheux problème moyennant un frais « de nettoyage » (« *scrubbing* ») somme toute, assez abordable (129 euros, ~ 200 CND). Toujours dans la même veine, il est possible de rémunérer des spécialistes pour noyer du contenu négatif dans une marée de contenu position afin de le reléguer beaucoup plus loin dans les résultats. Enfin, d'autres modèles douteux visent l'exploitation de rançongiciels.

Enfin, dans le *Darknet*, il existe également des marchés principalement destinés à la presse à scandale et aux paparazzi où il est possible de transiger des contrats portant sur des clichés ou

des informations spécifiques visant des individus en particulier. Chaque « commande » est rattachée à un prix et la somme n'est libérée que si un « intermédiaire de confiance » (« *escrow* » ou parfois sim-plement « escroc ») valide la transaction. Encore une fois, la nudité est l'élément le plus recherché, mais pas le seul. Par exemple, on peut y trouver des recherches plus sophistiquées telles « photos de personnalité *X* entre 30 et 40 ans » [430] ou « échantillon (de 300 mg ou plus) de l'ADN de *Y* » [431].

Modèles mixtes

Il y a également d'autres modèles d'affaires qui sont recensés dans la littérature et qui intègrent la GIDI ou la GIDIM dans leurs considérations et puisent des éléments dans plusieurs modèles.

Les modèles intégrés

En dernière note quant aux modèles d'affaires, il est pertinent d'attirer l'attention du lecteur sur les modèles dits « intégrés » où cette intégration s'exprime par le fait que le modèle intègre la fourniture de plusieurs services liés et, ce faisant, accroît l'influence de l'opérateur et la dépendance de l'utilisateur, ce qui s'explique par la portée bout-en-bout de cette influence dans ce contexte. Par exemple, divers opérateurs offrent des services musicaux tels « *Siren* », sur Public Mobile et Telus. D'autres, tel que mentionné précédemment, cherchent à devenir fournisseurs d'accès Internet. Dans tous les cas, il faut comprendre que bien que ces intégrations puissent améliorer la qualité du service, elles minent le principe de pluralité et d'indépendance des fonctions critiques, ce qui les rend plus sujettes à une éventuelle collusion, de là l'émergence de technologies anti-collusion.

2.5.2 Industrie de la GIDI – Valorisation des données – discussion générale des besoins

Les données que les utilisateurs génèrent valent leur pesant d'or. Il existe, à part entière, une économie des données. Celle-ci peut s'articuler positivement : la valeur attachée par diverses entités à la connaissance de certaines données; mais aussi négativement : la valeur attribuée par une partie *X* à ce qu'une partie *Y* (ou un ensemble de parties y_i, y_{ii}, etc.) n'ai(en)t pas accès à ces données. La valorisation négative peut être motivée par des considérations socialement perçues comme illégitimes (ex : infidélité conjugale), mais aussi pour des considérations politiques (appartenance à un groupe ou une mouvance politique) ou même louables et défendues par la Loi (orientation sexuelle, religion ou statut sérologique).

Au vu des modèles d'affaires présents en section [S: 2.5.1], il faut trouver un point d'équilibre entre les besoins assurant la viabilité de plusieurs modèles d'affaires qui pourraient être compromis par des changements trop radicaux, et les besoins légitimes des utilisateurs de ne pas être pistés sans répit. Il ne faut pas sous-estimer l'appât de la gratuité ou idéaliser l'importance accordée par les utilisateurs à leurs données. Il serait facile d'aborder un point de vue selon lequel nombreux sont ceux qui cèderaient des droits fondamentaux, dont ils ignorent souvent l'utilité, pour un maigre avantage, parfois insignifiant. Il ne faut pas sous-estimer l'importance des services « gratuits » dont en fait la survie dépend de l'acceptation sociale massive de ces conditions particulières en matière de vie privée. Il ne faut pas oublier non plus que nombreux peuvent être les cas où des données sont capturées, mais ne seront jamais utilisées. Ces sujets sont peu abordés dans la littérature académique. En ce qui concerne les préoccupations relatives à la vie privée, ainsi que leurs déterminants, ce sont les travaux académiques de Seounmi Youn (en 2009) [432] qui apportent une part substantielle des explications. Il serait intéressant de reproduire leurs activités de recherche puisque les données commencent à dater un peu. Du côté des préoccupations du côté des entreprises relativement à l'acquisition des données dont elles ont besoin, ce n'est pas dans la littérature académique, mais dans la littérature commerciale que les principaux éléments ont été trouvés. Ainsi, le rapport « *The struggles businesses face in accessing the information they need* »[282] aborde ce sujet. Notons qu'il fait état d'un taux d'à peine 26 % (environ un quart) des répondants qui affirment qu'ils utilisent toujours les données qu'ils amassent.

Si l'on désire proposer une amélioration à la situation actuelle, il faut comprendre en détail les motivations de parts et d'autres et proposer une situation où les besoins tant des uns que des autres sont conciliés. Il y a certes une sorte d'acceptation sociale qui s'est constituée au fil du temps, mais ce qui pose problème, ça semble être l'absence d'exceptions prévues ou de point intermédiaire. Pour arriver à cette conciliation, il faut d'abord sonder et comprendre chacune des principales les motivations, une à une, derrière les collectes de données, puis trouver pour chacune de ces motivations, des solutions acceptables lorsque c'est possible, le tout encadré par des principes applicables en tout temps.

Les motifs pour lesquels les entreprises peuvent collecter des données, parfois de manière outrancière, ne relèvent pas nécessairement de sinistres complots et de tables rondes des forces du mal. Dans certains cas, ceux qui engrangent ces données de manière indélicate peuvent le faire pour des motifs défendables, ou du moins, qui ne sont pas nécessairement hostiles. Ainsi, par exemple, les motifs suivants ont été recensés :

1) À des pures fins de télémétrie et instrumentation [283 à 288]
2) Pour mieux connaître les utilisateurs [290 èa 293]
3) Afin de se protéger juridiquement [294 èa 305]
4) Afin d'alimenter des algorithmes d'intelligence artificielle [306 à 316, 319]
5) Afin de faire progresser la science (ouverte) [317, 318, 320 à 325]
6) Dans le doute, vaut mieux capturer [326 à 331]

Ces faits saillants seront repris dans la section des résultats.

À elle seule, l'étude des motivations derrière ces captures de données pourrait faire l'objet d'un ouvrage académique en soi. Il n'est donc pas question ici d'approfondir le sujet, mais de survoler la logique des arguments.

1) À des pures fins de télémétrie et instrumentation

Ici, ce sont essentiellement des logiciels à code source ouvert et qui sont opérés par des fondations ou des collectifs ou des groupes de bénévoles qui se classent généralement ici. Ce

sont, pour la plupart, des logiciels qui nécessitent une certaine interaction avec l'utilisateur et les données qui sont capturées et transmises sont souvent de nature inconnue, elles constituent des captures récentes de l'état des diverses variables du programme avant la défaillance. Pour ce motif, l'OAS ne sait pas d'avance ce qu'il va recevoir. Il se peut que ce soit des données sur une recette de salade de haricots ou bien un message ultra personnel et ultra compromettant d'une personnalité importante. Ce type de capture n'est associée qu'à un intérêt très limité à rattacher l'identité d'un individu aux données, sauf si besoin est de le joindre pour régler le problème ou avoir plus de détails. Cependant, il peut y avoir un intérêt légitime à associer aux données l'identité d'un appareil. En ce sens, une solution proposée peut être de garder le tout en son état actuel, mais d'effectuer des filtrages sélectifs sur des données spécifiques : noms, prénoms, numéros de téléphone, etc. Ce n'est certes pas une défense à tout épreuve, mais ça constitue un pas dans la bonne direction.

2) Pour mieux connaître les utilisateurs

C'est ici que la posture est la plus questionnable. Il y a un certain mélange de curiosité naturelle, de voyeurisme et de recherche d'opportunité d'affaires. Souvent, la capture de données sert à tenter de faire face à un vide ou à une impasse sur le plan stratégique. Ainsi, l'opérateur de l'application peut se demander comment il peut améliorer son offre de services, connaître les tendances des utilisateurs ou maximiser la valeur de sa compagnie dans l'optique d'une éventuelle revente. À cette préoccupation, il est difficile d'apporter un compromis directement applicable. Une partie de la solution peut provenir du fait qu'il y a peu de valeur dans les données individuelles et personnelles, puisque la valeur se trouve davantage dans les tendances. À cet effet, divers filtres sur champs peuvent être appliqués afin de ne recueillir que les données dépersonnalisées. Évidemment, ce genre de mesure peut facilement d'une désanonymisation.

3) Afin de se protéger juridiquement

Certains développeurs conservent ces données afin de se rassurer face à des risques juridiques ou réglementaires. Ce sont les opérateurs d'applications et services qui sont les plus préoccupés par leur obligation de collaboration auprès des autorités et de conservation de

données dans des cadres qu'ils considèrent risqués. Par exemple, des entreprises conservatrices qui se lancent dans le domaine des cryptomonnaies peuvent avoir une telle attitude afin de démontrer leur plus soumise et entière collaboration et se laver les mains des comportements de leurs clients. Une telle attitude de prudence révèle souvent une mauvaise compréhension du contexte juridique applicable, de leurs réelles obligations et des procédures judiciaires en place ainsi que le déploiement dans une multitude de juridictions non-harmonisées. Concernant cette motivation, le mieux serait d'impliquer les organismes réglementaires avec le concours du Commissaire à la vie privée, afin de proposer des cadres fiables aux opérateurs d'applications ou de services, de manière à réduire l'incertitude qui mène à cette collecte tous azimuts.

4) Afin d'alimenter des algorithmes d'intelligence artificielle

Parmi les raisons les plus compréhensibles, celle-ci semble être la plus populaire. Ainsi, ce sont surtout les captures en vue de fournir des ensembles de données d'entrainement aux algorithmes de reconnaissance vocale de Google [315] et de *Facebook* [314] qui ont défrayé la manchette puisque ces captures s'opéraient parfois à l'insu des UFs. La préoccupation, de part et d'autres est compréhensible. D'une part, les besoins sont énormes en volumes de données nécessaires pour parfaire un algorithme. D'autre part, les citoyens peuvent ne pas vouloir être épiés.

À ce chapitre, une des questions à se poser est définitivement celle concernant les limites de la discrimination éthiquement acceptable par les machines [319]. Si, par exemple, un système intelligent venait à dresser une corrélation entre ethnie et criminalité ou bien entre emploi et condition de santé, il faudrait savoir quelle utilisation serait constitutionnellement admissible à l'égard de ces conclusions.

Notons par ailleurs que la littérature dans ce domaine fait référence aux données par l'allégorie de la « mine », comme étant une sorte d'actif public, mais réellement sans propriétaire et duquel tout un chacun qui réclame un droit de forage, aussi ténu et rudimentaire soit-il, dispose de la prérogative de s'y enrichir. Or, cela évacue du discours toute éventuelle propriété des données dérivées que pourrait avoir l'émetteur (et souvent le

sujet) des données initiales. Peut-être faudrait-il aller plus loin avec l'analogie de la mine et subordonner son exploitation à une réglementation (restrictive cette fois-ci) et à un système de redevances payables à tous et, par défaut, à l'État?

5) Afin de faire progresser la science (ouverte)

Parmi les raisons discutables, celle-ci semble la plus louable. Sunyoung Kim et Jennifer Mankoff ont étudié (2010-2015) [321 à 325] ce phénomène dans un contexte de contrôlé. Bref, c'est assez peu répandu, mais l'argument est valable. Les principaux éléments de l'argument sont à l'effet que les données capturées (à l'insu des utilisateurs ou presque) sont plus fiables que celles recueillies par des questionnaires. Il est à noter que dans ce cas, les données n'ont pas besoin d'être liées à des identités et que l'échantillonnage permet de se satisfaire de fiablement avec des données moins volumineuses.

6) Dans le doute, vaut mieux capturer

Enfin, une réponse souvent rencontrée, mais qui n'en est pas réellement une, est celle voulant que l'on serve les données parce que l'on ignore ce qu'elles pourraient un jour révéler comme connaissances utiles et valables dans un futur éloigné. Notons que ces réponses coïncident avec des scores plus bas aux questions de sécurité de l'information dans des versions antérieures du présent mémoire. Bref, cette attitude tend à trahir un manque de préparation et d'organisation dans l'exploitation des données. Sur ce dernier type de souci, la meilleure parade est probablement l'éducation et la sensibilisation.

2.5.3 Risques relatifs aux données

Les principaux risques identifiés relatifs aux données s'articulent autour de la triade de la sécurité :

1) Intégrité

La corruption des données ou leur altération dirigée sont les principaux risques. En ce qui concerne les données personnelles ou celles liées à la GIDIM, ce sont essentiellement les risques liés à l'usurpation ou la suppression d'identité qui s'articulent dans cet ensemble. Ce risque est facilement mitigé par des mesures de contrôle de l'intégrité, tels les hachés cryptographiques, les certificats, les signatures numériques et les services de validation externe.

2) Disponibilité

L'indisponibilité des données d'identité peut mener à l'incapacité d'exercer ses droits citoyens, à la compromission de sa personnalité juridique et à l'adoption de mesures alternatives opposées à l'état de droit. Par exemple, si un état venait à rendre indisponibles les identités de tous les citoyens n'ayant pas acquitté tous leurs dus (impôts, amendes, etc.), une progression de l'activité en absence de l'identité formelle pourrait être à craindre. Un cas précis pourrait être celui du travail dissimulé qui pourrait se voir exploser si les contrevenants ne pouvaient plus toucher les allocations ou se trouver un emploi déclaré, ce qui alimenterait un cercle vicieux. Quant à elle, l'indisponibilité de données personnelles revêt principalement les formes des défaillances fortuites (accidents), systémiques (erreurs à grande échelle) ou volontaires (ex : rançongiciels).

3) Confidentialité

La confidentialité, quant à elle, est l'élément le plus connu et intuitif de la triade de sécurité. Elle regroupe l'ensemble des risques relatifs aux fuites de données ainsi qu'aux accès non-autorisés à celles-ci.

Ces trois principaux types de risques ayant été identifiés, il faut garder à l'esprit que, peu importe qui sera le fournisseur de services de GIDIM, celui-ci devra assumer la tâche importante d'assurer un niveau de sécurité suffisant en lien avec les risques identifiés ci-haut. Le principal de la difficulté décrite en introduction est d'analyser le sujet de manière

académique, ce qui requiert de fixer un cadre volumineux de construits, puis de concepts nécessaires à une étude rigoureuse de cette réalité complexe.

À ce stade, on a défini l'identité et ses données ainsi que la GIDIM. On a présenté les cadres applicables, les intérêts et les modèles d'affaires établis, ainsi que les risques et les parties impliquées. L'échiquier est à ce stade garni, le jeu peut commencer.

2.6 Dérapages possibles et principaux risques à envisager

Cette sous-section se veut brève, car elle demeure spéculative et ne vise qu'à identifier les principaux risques qui se dégagent au constat des modèles d'affaires et des inadéquations constatées dont les solutions seront documentées ultérieurement.

En l'espèce, le principal risque est celui de voir les rapports de pouvoir se reproduire, voire s'aggraver, entre l'UF et les différents opérateurs.

Bien qu'il y ait une concurrence entre les joueurs, il y a une situation d'oligopole et un autre risque est celui d'abus d'oligopole.

Enfin, de par l'importante collecte de données qui s'opère et qui est même enchâssée dans plusieurs modèles d'affaires, il y a risque de perte de toute vie privée et de développement d'une position vulnérable, prévisible et ainsi fragilisée des UFs tant face aux opérateurs qu'à leurs partenaires et à l'État.

Ce sont essentiellement à cet égard que seront orientées la plupart des améliorations proposées.

2.7 Étude approfondie de produits

Au sujet des plateformes existantes et de leur analyse : cette section (et ses sous-sections) comporte une description des principales plateformes existantes, se limitant essentielle aux plus connues et mettant une emphase particulière sur les deux principales, *iOS* et *Android*..

2.7.1 Plateforme *Apple* telle que rapportée dans la littérature

Cette sous-section a comme particularité d'étudier un cas peu commun, sujet à des réserves qui doivent être communiquées. Elle vise à étudier la plateforme Apple telle que décrite dans la littérature. Or, de par les clauses contractuelles qui régissent les activités techniques (développement d'applis, action en tant que partenaire, etc.) ainsi que la simple utilisation de leurs produits, *Apple* décourage et limite grandement la production de matériel externe et indépendant, à leur sujet. Donc, l'essentiel de la « littérature » décrivant les produits *Apple* provient d'*Apple* ou d'une communauté très favorable (que certains appellent plus ou moins moqueusement « la secte [430] *Apple* »).

Donc, la plateforme de distribution pour *iOS* dispose d'un contrôle plus ferme sur la diffusion des applications que sa rivale pour *Android*. Tout d'abord, il y a monopole et validation du matériel de manière à assurer une uniformité dans le fonctionnement et la performance ainsi qu'une authenticité des logiciels et licences et du matériel sur lequel ces logiciels sont appelés à fonctionner. En ce sens, il est possible, quoique très rare, de trouver des téléphones *Apple* contrefaits avec *iOS* et, de toutes manières, les mises à jour ont tendance à les rendre inopérants. Les rapports serrés entre *Apple* et son fournisseur Foxcon (*Hon Hai Precision Industry Company Ltd.*) sont connus et favorisent le monopole de fait et de droit d'*Apple* sur le matériel produit sur mesures et de manière exclusive. Cela distingue le cas mobile du cas Mac (ordinateur de bureau) où les pièces essentielles sont facilement disponibles à quiconque, ce qui permet notamment de monter des versions apocryphes (appelées « *HackIntosh* ») [332]. Toujours côté matériel, un problème subsiste néanmoins et il s'agit des pièces et accessoires non-autorisés. Ceux-ci réussissent parfois à contourner diverses mesures de contrôle de l'authenticité des pièces lorsqu'il y en a, bien que la plupart du temps,

seules certaines pièces soient munies de telles mesures. Étonnamment, l'écran et le panneau tactile sur lequel il est superposé ne font pas l'objet de telles mesures alors qu'ils sont parmi les composants les plus souvent endommagés et remplacées. D'autres dispositifs tels les câbles de connexion USB ou vidéo sont pourtant protégés par de telles mesures [332, 333 et 334]. Notons que les schémas électroniques (« *schematics* » ou « *blueprints* ») officiels ne sont pas disponibles.

Il y a ensuite une deuxième couche de contrôle qui se situe au niveau du système d'exploitation, *iOS*. Ce système n'est pas en code-source libre, mais certaines des fonctionnalités sur lesquelles celui-ci repose le sont et leur source doit donc être publié. À ce stade, c'est la sécurité opérationnelle qui vient en renfort, principalement au travers des vérifications des certificats de sécurité. À moins de changement manuel et profond, il y a deux catégories de certificats de sécurité : ceux servant à la diffusion d'applications via l'*AppSotre* et ceux servant à d'autres fins, tels la communication via SSL. Les certificats pour la distribution d'applications doivent être signés par un *Apple* ID valide et c'est là que la sécurité opérationnelle rentre en ligne de compte.

Tout d'abord, la sécurité opérationnelle dicte le fait que chaque appareil doive être enregistré à une identité plausible et qu'il y ait diverses restrictions sur ce qui peut être mis comme nom et prénom, ou numéro de téléphone. De plus, en cas de problèmes, il faut avoir une adresse courriel valide (ou en créer une sur *iCloud*, ce qui en requiert une également) afin de pouvoir communiquer avec le *Genius Bar* du magasin *Apple Store* du choix de l'utilisateur.

Or, la sécurité opérationnelle pour la distribution d'applications est absolument plus complexe. Tout d'abord, pour accéder au kit de développement, il faut faire partie du programme de développement, ce qui requiert une ouverture de compte et des frais annuels. Lors de l'ouverture de compte, il est possible de s'enregistrer en tant qu'individu ou qu'entreprise (ou que grande entreprise dans le cadre d'un contrat particulier avec *Apple*). Dans le cas d'un enregistrement individuel, il faut fournir des copies des pièces d'identité. Dans le cadre d'un enregistrement corporatif, il faut présenter une copie des papiers d'incorporation ainsi que des pièces d'identité de chacun des administrateurs. De plus, le nom d'éditeur devra correspondre de manière exacte au nom officiel de la compagnie, même pour

les tests. De plus, si un éditeur désire rentabiliser son application au travers des publicités, des frais ou d'un coût de vente (sur l'*AppStore*), il faut également communiquer et tenir à jour les données bancaires. L'enregistrement comme grande entreprise permet notamment de distribuer localement des applications, jusqu'à cinquante (50) appareils à la fois (par identité) par installation directe (USB ou système « *Push* ») aux appareils de l'entreprise ou de partenaires.

Bref, l'identité et les coordonnées bancaires des opérateurs de plateformes applicatives sont connues par *Apple*. Cela fait partie intégrante (et constitue un des principaux éléments) de la stratégie de sécurité d'*Apple* : établir un cadre sécuritaire d'informatique dite « de confiance » (« *trusted computing* ») [335 et 336], mais possiblement sans le TCG. Notons qu'*iOS* est une forme d'Unix.

Certes, il est possible de contourner l'ensemble des mécanismes (ex : avec la technique de « libération des verrous » (« *jailbreaking* », plus de détails en [S: 2.7.6]). Or, cette technique est connue et, de l'opinion d'*Apple*, elle est contractuellement interdite et son adoption était suffisante, selon Apple, pour mettre fin à toute garantie ou clause protective, ce qui a posé initialement des contradictions avec certaines protections législatives [337 et 338]. Il est également possible d'agir avec un peu plus de stratégie et simplement remplacer des éléments racine dans la pyramide des certificats SSL. Bien que le système produise plusieurs avertissements pendant cette manipulation, cette option est permise. Ensuite, il est possible d'interférer directement sur la mémoire vive et sur les contrôleurs réseaux afin d'intégrer des intergiciels tels Sekomon, Tivoli ou d'autres. Notons que les applications sont développées en langage Cocoa pour les plateformes *iOS*. Or, Cocoa repose sur l'Objective-C, la compilation directe en langage C est permise. Par ailleurs, elle permet d'atteindre des performances très intéressantes et cette option semble volontairement laissée disponible pour le développement de jeux et d'applications faisant usage d'OpenGL ou de Cuda.

À sa base même, *Apple* mise sur la conformité, laquelle se veut le respect strict d'états exclusivement autorisés, ce qui limite le champ des possibles. Notons que l'identité étant définie comme un ensemble d'attributs permettant de différencier, la conformité fait office de facteur de contraste. Par analogie visuelle, si l'identité est la couleur d'un trait sur un dessin,

la conformité est une norme rendant l'arrière-plan uniforme, ce qui fait ressortir cette couleur du trait.

Sur le plan technique, cette conformité se traduit par des mises à jour obligatoires, même lorsqu'elles sont problématiques, ainsi que par un profil de risque moins diversifié, qui privilégie d'assumer un risque faible que tous les utilisateurs soient touchés par une seule faille (qu'il sera urgent de colmater) à devoir suivre plusieurs failles potentielles à risque encore plus faible, chacune ne touchant qu'une portion du parc d'appareils. De manière inhérente, cela repose sur une foi absolue envers la capacité des ingénieurs de l'équipe de réponse aux incidents chez *Apple* d'élaborer une parade ou un correctif dans des délais utiles.

Toujours, sur le plan technique, l'appareil *iPhone* est conçu strictement comme un appareil personnel et même le prêt est conditionnel à l'acceptation par l'individu à qui il est prêté, des nombreux termes et conditions. La stratégie en matière de GIDIM est très limitée, car il y a un monopole, celui d'*Apple*, lequel ne se voit pas céder sa place en tant qu'autorité centrale. Tout repose donc sur l'*Apple* ID et les OAS sont invités à bien vouloir dépendre des services d'identité développés autour de l'*Apple* ID. Même s'ils déclinent, au niveau de la couche système, cet identifiant aura le dessus et toute gestion de données par les applications ne pourra être que subordonnée aux paramètres du système.

Tel que mentionné au point [SE : 1.3], d'un point de vue technique, l'importance d'affaires que présentent l'*AppStore* et *iTunes*, ainsi que les services comme *Apple*TV sont autant d'incitatifs pour *Apple* à renforcer sa sécurité, en particulier contre les risques d'extraction de contenu. Le risque ultime serait de voir un dispositif matériel ou logiciel capable d'extraire en format libre de DRMs, les chansons ou vidéos achetés au travers *iTunes* ou les applications achetées au travers de l'*AppStore*. Une telle extraction permettrait, du moins dans le cas du contenu non-exécutable, d'avoir des fichiers source de haute qualité qui pourraient être partagés via des réseaux de partage de contenu protégé, dont ceux de pair-à-pair tels ThePirateBay. Pour parer à cette éventualité, *Apple* emploie des techniques de stéganographie afin de pouvoir retracer éventuellement l'identité à laquelle serait rattaché le contenu ainsi partagé.

Devant ce risque, des choix structurels ont été pris, notamment celui de compartimenter l'accès par application. Ainsi, chaque application ne peut communiquer avec les autres qu'au travers de certaines interfaces programmatiques (APIs) clairement et précisément définies et encadrées. Une application ne peut pas accéder aux données des autres applications et il n'y a pas d'espace de données commun, c'est pour ce motif qu'il n'est pas possible d'avoir une application de sauvegarde ou d'exportation de fichiers. Seules les interfaces disponibles au niveau système permettent de tels accès. Cela confère donc à *Apple* le monopole sur l'exportation des données à partir du téléphone.

Ensuite, les applications font l'objet d'une approbation avant d'être publiées sur l'*AppStore*. Lorsqu'un développeur est une grande entreprise, il peut court-circuiter le processus d'approbation, mais uniquement pour un ensemble d'appareils rattachés à son identité, dont la taille ne peut dépasser cinquante (50) appareils, toute catégorie confondue. Cela permet notamment les fonctions de test. Pour le commun des développeurs, il faut attendre que les représentants d'*Apple* procèdent à l'inspection tant du code que du produit fini pour donner leur autorisation à rendre l'application exécutable et apte à la distribution. L'application soumise doit obligatoirement être signée. Au surplus, elle doit être conforme aux normes dictées par *Apple*, notamment en matière d'ergonomie, de fonctionnement et de visuel. L'argument mis de l'avant est de s'assurer d'avoir un ensemble d'offre de produits (Applis) uniforme et de qualité. L'obtention de l'approbation n'est pas un droit, mais un privilège et elle peut être révoquée à tout moment, elle peut même faire l'objet d'un retrait a posteriori, au travers le « *killswitch* ». Outre les aspects visuels et d'ergonomie, *Apple* étant souveraine en matière d'approbation, des considérations d'affaires peuvent disqualifier par rapport au processus. Ainsi, Firefox et *Opera* ont été recalés [339 à 342] de l'*AppStore* du simple motif qu'il y avait déjà un logiciel (Safari, par *Apple*) qui offrait le même service, fonctionnalité ou capacité applicative (navigation web), ceux-ci étant alors considérés comme redondants. Il n'est pas difficile d'y percevoir une simple argutie de protection de son monopole.

Cette rigidité rend compliqué le déploiement de certains types de logiciels. Une emphase particulière serait de mise, sur ce sujet, à l'égard des intergiciels, lesquels sont, de par la nature

même de leur conception, incompatibles avec la philosophie de génie logiciel selon *Apple*. En particulier, les déploiements d'intergiciels de GIDIM et de MDM s'avèrent particulièrement fastidieux. Depuis la version *iOS* 7, en fait, encore une fois, c'est le système qui s'arroge le monopole et la gestion des parcs d'appareils mobiles se fait au travers une interface dédiée et conforme à un protocole « *MDM Protocol* ». *Apple* offre un service « *Device Enrollment Program* », lequel permet d'automatiser plusieurs aspects de la gestion. Or, il semble être conçu pour fonctionner de manière optimale avec un parc constitué exclusivement de dispositifs *Apple*, et induire donc ainsi un tropisme favorable à la migration vers le tout-*Apple*.

Exemple de contenu de message sous protocole MDM :

```
HTTP/1.1 200 OK
Content-Length: 1234
Content-Type: application/xml; charset=UTF-8
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.Apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
  <dict>
    <key>CommandUUID</key>
    <string>9F09D114-BCFD-42AD-A974-371AA7D6256E</string>
    <key>Command</key>
    <dict>
     ...
    </dict>
  </dict>
</plist>
```

Insertion 3.1 (code source) – Source : Mobile Device Management Protocol Reference [343]

Voilà des facteurs qui tendent à limiter l'utilisation d'appareils *iOS* dans le cadre d'une utilisation en entreprise et c'est la concurrence qui profite de cette faiblesse.

Par ailleurs, concernant la prise de position au travers sa lettre aux clients, *Apple* assure qu'elle est prête à défendre jusqu'en Cour Suprême les droits de ses utilisateurs en refusant, lorsqu'elle le juge injustifié, de se conformer à certaines demandes de la part des autorités gouvernementales. Elle s'est également rangée dans le groupe des intervenants en défaveur

de la proposition quelque peu naïve des autorités cherchant à obliger les OPs à introduire des portes dérobées au seul usage des États.

Ce n'est pas la première fois que les autorités visitent une telle approche architecturale. Les motions ClipChip et les lois et règlements sur le contrôle des exportations (« *Export Administration Regulations* », « *EAR(s)* ») ont sondé cette option. Une étude rigoureuse de la question technique permet de déceler deux versions à cette approche. La première étant celle de l'affaiblissement, la deuxième étant celle de la fonctionnalité spécifique. De manière classique, ce que la plupart des intervenants politiques exigeaient a davantage ressemblé à une stratégie d'affaiblissement, ce n'est que récemment que la stratégie de la fonctionnalité spécifique est dûment étudiée et cela peut être du à l'évolution de la connaissance disponible aux décideurs politiques, et à l'ensemble du public, relativement à cette question. Cette partie du débat concerne d'ailleurs toutes les plateformes.

D'abord, la stratégie de l'affaiblissement se rapproche de certaines décisions qui ont été prises par la NSA, qui pourtant doit veiller sur la sécurité des communications des Américains, de ne pas toujours agir de manière à optimiser cette sécurité, dans le but de préserver un accès praticable. Cela peut prendre diverses formes : promouvoir un algorithme cryptographiquement faible (à basse entropie [344 et 345] ou à conception peu robuste), ne pas apporter des correctifs à des problèmes connus et pour lesquels la solution a été trouvée, disséminer des fausses croyances ou connaissances, etc. Toutes ces stratégies ont comme résultat d'affaiblir les systèmes que l'on tente de sécuriser et ces faiblesses peuvent être exploitées par tous ceux qui connaissent la vulnérabilité et qui savent l'exploiter. Une telle stratégie est basée sur la présomption que celui qui l'emploie dispose d'un accès privilégié à cette faille de manière suffisamment importante pour que le risque en vaille l'avantage. Plus concrètement, une agence spécialisée peut être d'avis que la faille est subtile et qu'il est peu probable de la trouver, même si le code source est public. Le fait d'être le seul à la connaître dépend entièrement du secret, ainsi que de la basse probabilité de découverte indépendante par une tierce partie. Sur ce dernier point, une telle agence peut présumer que ses moyens techniques et humains peuvent lui donner un avantage considérable. Or, cette perspective pose de nombreux problèmes. Tout d'abord, il y a la découverte aléatoire par un simple développeur ou analyste, local ou étranger, qui se trouve au bon endroit au mauvais moment.

L'approche classique est, si celui-ci se trouve sous la sphère d'influence (territoriale) de l'agence, de s'assurer de sa discrétion par divers moyens, dont l'intimidation peut notamment en être un pertinent à étudier. Ensuite, il faut considérer la professionnalisation des activités de piratage, notamment par le crime organisé. Ainsi, la faille *Eternal Blue* (CVE-2017-0144) [346] qui était apparemment connue par la NSA [347] a été exploitée par des pirates afin de permettre des attaques de rançongiciel, *WannaCry*. Cela rappelle le cas de *Heartbleed* [348 et 349]. À ce chapitre, le développement d'outils d'analyse formelle ou apprenante du code source [350 à 353] permet de révéler plusieurs de ces failles, au travers des modélisations déterministes ou probabilistes. Il existe même des projets d'intelligence artificielle développés afin de relever de telles vulnérabilités. Enfin, il faut considérer que des nations concurrentes, voire ennemies puissent disposer de moyens capables de trouver la faille en question et de l'exploiter, malgré le fait que leur taille et leur budget soient considérablement plus restreints.

De l'autre côté, il y a la proposition de l'installation d'une fonctionnalité spécifique d'accès, laquelle serait une extension aux normes *CALEA* et similaires déjà en place auprès des OTs, favorisant l'interception autorisées à l'intérieur du cadre juridique. Une telle approche n'est pas étudiée et la plupart des commentaires techniques se rabattent sur la stratégie d'affaiblissement, sans se concentrer sur cette option. Une telle fonctionnalité donnerait un accès, en bonne et due forme, à une autorité légitime, à un ensemble de données. La première question à étudier sous cette avenue serait de la couche (voir section [S: 2.3.5] pour une meilleure compréhension) au travers laquelle cela devrait être mis en œuvre. Cela pourrait être mis en œuvre au niveau application, ce qui requiert à chaque application de disposer d'une telle interface et qui déplace quelque peu la responsabilité de conformité au niveau de l'OAS et non de l'OP, en plus de modifier et segmenter légèrement les risques. Il serait aussi possible de mettre en œuvre cette fonctionnalité au niveau « session », donc une fois que les mécanismes de GIDIM s'assurent de l'identité de l'individu. Or, cela serait sous-optimal puisqu'il suffirait de changer l'identité de l'utilisateur pour déjouer le dispositif.

Enfin, cela peut être mis en œuvre au niveau système, ce qui semble optimal. Une fonctionnalité d'accès au niveau système pourrait demander de cataloguer et formaliser les types et structures de données des applications si l'on désire une meilleure granularité. En

absence de granularité, c'est un ensemble de données plus large et moins structuré (plus judiciaire, « *forensic* », brut) qui transiterait, ce qui exigerait plus de bande passante et qui risquerait de rendre la camouflage de tels transferts moins facile et, au bout du compte, augmenter le risque que l'opération soit compromise parce que la cible s'est rendue compte de la surveillance. Il faudrait aussi modéliser les exigences que peut exprimer un tribunal et automatiser le tout (ex : envoyer les données de géopositionnement à chaque lundi, 17h00 GMT -05:00). Cela aurait également des impacts sur la performance des appareils.

Outre les considérations techniques, il y aurait aussi des considérations de gestion à apprécier. Si la technologie existe et qu'elle est incluse dans les appareils, dans chaque juridiction où c'est le cas, la justice pourrait exiger de l'OP ou de l'OAS d'activer la fonctionnalité selon les paramètres qu'elle juge opportun. Cela ouvre la porte à des conflits de juridiction, notamment à cause de l'extra-territorialité de certaines lois et tribunaux. Par exemple, l'OP ou l'OAS pourrait se voir contraint à donner accès à ces fonctionnalités à un État comme l'Iran, auprès d'une cible militante des droits humains, laquelle pourrait ensuite faire l'objet de torture ou de mauvais traitements. Ce faisant, il expose sa responsabilité, notamment auprès des organismes qui sont nationaux ou internationaux (ex : cours fédérale du Canada) susceptibles de tenir l'OP ou l'OAS responsable de violations de droits humains (par complicité) ou de crimes sous le droit international et contre lesquels le droit national n'est d'aucune utilité ou secours comme justification disculpatoire des agissements.

Officiellement, la position d'*Apple* est à l'effet qu'elle est volontairement incapable de casser la sécurité des données résidant sur le téléphone. Cela ne la préclut cependant aucunement sa capacité d'accéder à des données recueillies à même le téléphone, tels le géopositionnement, ou bien les données sur *iCloud*, incluant les photos. Enfin, cela n'empêche pas le OT de partager les données relatives aux télécommunications, au surplus des métadonnées, lesquelles sont communiquées de manière automatique. Ce qui rend possible, architecturalement, pour les États d'accéder aux données de géopositionnement comme c'est le cas dans le dossier du journaliste Patrick Lagacé, c'est que l'opérateur lui-même a accès à ces données, et ne peut donc se soustraire à l'obligation de les partager. Il faut observer au passage, que le dénouement du dossier opposant le FBI à *Apple* (cas San Bernardino) est apparemment dû au fait qu'un expert (pirate) ait offert au FBI une option lui permettant

d'arriver à ses fins par une voie technique, plutôt que par une voie légale, ce qui permet d'éviter le débat constitutionnel sur la question (pour le moment) et qui coûte probablement moins cher également. Cela permet donc de conclure qu'une vulnérabilité technique existe qui permet l'extraction de ces données sans l'apport d'*Apple*.

Voilà donc résumés les motifs pour lesquels certaines intrusions sont architecturalement possibles et d'autres ne le sont pas, sur la plateforme *iOS*, ainsi que les avenues qui ont été considérées, et acceptées ou rejetées, ainsi que celles qui sont ou seraient exploitées afin de permettre la communication de certains renseignements aux autorités étatiques compétentes.

Résumé des modèles d'affaires imputables à *Apple*

On peut comprendre que les modèle d'affaires exploités par *Apple* ressemblent surtout à ceux de vente d'appareils, de licences individuelles et de services, tout en n'offrant qu'un contrôle très limité aux UFs. La particularité de ce modèle : investir massivement dans la publicité afin de préserver le caractère désirable de l'appareil, notamment au travers des efforts de valorisation de marque.

Au niveau de la rétention de la clientèle, il est clair qu'au vu des investissements nécessaires au développement de cette clientèle, il est probable qu'*Apple* soit incité à ne pas la laisser partir, au contraire, *Apple* a développé des outils permettant la migration, mais seulement dans l'autre sens, depuis *Android* vers Google, profitant du caractère ouvert de son concurrent, ce qui rend la riposte plus compliquée du fait que *iOS* n'est pas aussi ouvert.

Notons également que l'ensemble des politiques et conditions permettent de conclure qu'*Apple* entretient une crainte très prononcée vis-à-vis l'idée de voir surgir des plateformes alternatives qui soient capables de fonctionner sur son matériel, bref de perdre le contrôle sur la conformité.

Enfin, notons que le contrôle qu'oppose *Apple*, notamment en matière de vérifications à l'effet que le logiciel ne soit pas altéré peut entrer en conflit avec diverses provisions

législatives qui permettent une jouissance pleine et entière, dont en matière de garantie, notamment, aux États-Unis, le *Magnuson–Moss Warranty Act* de 1975 [338].

Les principales caractéristiques d'Apple ayant été rapportées, telles que recensées dans la littérature, ici est arrivé le tour de présenter les caractéristiques de la plateforme *Android*, également, telle que recensée dans la littérature.

2.7.2 Plateforme *Android* telle que rapportée dans la littérature

La sécurité d'*Android* repose sur un modèle complètement différent d'*Apple*. Il n'y a pas de contrôle obligatoire de l'identité par l'OP, ce qui ouvre la porte à ce que ce soit un véritable bazar. De plus, attendu qu'une partie importante du code est ouvert (« *open source* »), il est plus probable que des problèmes soient trouvés par des spécialistes ou des utilisateurs malicieux.

Enfin, attendu que Google ne contrôle pas la production du matériel (et permet même la virtualisation) pour les appareils roulant sur *Android*, l'analyse peut être poussée beaucoup plus loin, de même que la recherche de vulnérabilités ... et de correctifs.

Malgré tous ces motifs militant *a priori* à l'effet que la sécurité sur *Android* puisse être moins bien garantie, il semblerait que ce soit tout le contraire. Cela a notamment valu à cette plateforme d'être apparemment la seule sur laquelle l'agence américaine de la sécurité nationale « *National Security Agency* » ait investi des efforts considérables en recherche et développement, principalement centrées autour de la sécurisation des appareils mobiles, au travers diverses initiatives, le plus souvent pilotées par Stephen Smalley.

En fait, *Android* est une version spécialisée du noyau (« *kernel* ») Linux avec des fonctions minimalistes. Il existe trois autres versions spécialisées de Linux qui semblent pertinentes en matière de GIDIM : Docker/Qubes, Tails et SELinux. Les travaux de Smalley font suite aux travaux de Nakamura qui visaient à porter SELinux dans un environnement traditionnellement réservé à Linux Embedded. L'idée était de rendre SELinux disponible sur

des plateformes mobiles avant même l'arrivée du *iPhone*. Cette idée a repris de la pertinence avec l'arrivée des séries N800 de Nokia qui opéraient sur Linux Debian. Ensuite, *Android* a carrément envahi le marché et les efforts de recherche se sont tournés en ce sens.

L'expert en la matière provient du laboratoire *EPOCH* de l'armée américaine. Il a ensuite travaillé dans divers laboratoires de la *National Security Agency*, toujours apparemment sur le même projet, SE*Android*. À cet égard, il y a une prise de position importante de la part de la NSA en saisissant les opportunités offertes par le fait qu'une partie importante du code source d'*Android* soit ouvert et cela semble faire suite aux efforts canadiens de coopération entre Blackberry (une corporation canadienne) et le Centre pour la sécurité des télécommunications (du Canada, CST, le pendant canadien de la NSA). La présente section détaille une partie des travaux de cet auteur (Smalley) entre 2009 et 2016.

Son article décrivant en détail le mieux ses travaux a été produit en 2014 et s'intitule « *Security Enhanced (SE) Android: Bringing Flexible MAC to Android* » (Smalley, 2014) [354]. Il s'agit de son article en format scientifique le plus cité et depuis, la plupart de ses travaux prennent désormais plutôt la forme de présentations Powerpoint (en PDF) portant sur des (sous-)sujets spécifiques.

Les travaux de Smalley peuvent se résumer en cinq volets : adapter *Android* à SELinux en ajoutant des structure intermédiaires, jouant en quelques sorte des fonctions d'intergiciel (ex : offrant notamment la possibilité d'utiliser les descripteurs de sécurité sur le système de fichiers); basculer d'une approche de « contrôle d'accès discrétionnaire » vers une sous le type de « contrôle d'accès obligatoire »; développer les politiques qui manquent pour pouvoir mettre en œuvre ce nouveau modèle de contrôle et tester la viabilité et la pertinence de la mise en œuvre, principalement sur les aspect relatifs à la performance (et à la perte de celle-ci) et au gain d'efficacité dans la capacité d'empêcher des attaques, principalement des élévations de privilèges. Notons qu'une partie des travaux vise à relever des défis provenant du fait qu'*Android* n'a pas été conçu sous le paradigme de contrôle d'accès obligatoire et qu'à certains égards, notamment en matière de connectivité, des situation cocasses peuvent survenir du fait de ces lacunes de conception.

L'analyse réalisée par Smalley (« *Security Enhanced (SE) Android (...)* » et suites) est très poussée, notamment en ce qui a trait aux opérations qui ont lieu lors de la création de processus sur *Android*. Cette analyse met en évidence l'attribution des propriétés et des accès en mode ordinaire, comparées en mode SELinux. Notamment, ces travaux mettent en évidence le fait que chaque application dispose d'accès basés sur les comptes linux et que chaque éditeur signant ses applications de manière similaire peut les faire rouler sous les mêmes identifiants d'utilisateur ou de groupe (uid ou gid). Une bonne partie de la sécurité sous *Android* repose sur la capacité de segmenter ces accès, surtout au travers du système de fichiers, *aufs*, cependant connu comme plutôt déficient. Or, il y a des zones partagées et des interfaces de communication. Les travaux ultérieurs de Smalley portent sur des techniques d'isolation de ces groupes d'utilisateurs ainsi que sur la subordination de ces zones communes à des politiques obligatoires de sécurité. Dans ses travaux les plus récents (de mai 2016) [355] portant sur *Android* 5.0 et 6.0, les sujets abordés visent principalement la coordination des segmentations de manière à permettre non seulement d'avoir des « *utilisateurs* » distincts au niveau du système (Linux), mais également des utilisateurs distincts au sens de la GIDIM, des individus ou des contexte individuels distincts. Un constat se dégage des travaux de Smalley et c'est la volonté de promouvoir l'idée d'avoir un nombre fixe et limité d'identités à un instant *t*, lesquelles ne peuvent pas se créer à volonté, et que chacune de ces identités soi sujette à une politique de contrôle d'accès obligatoire.

Cela peut sembler politiquement intéressant, en particulier si l'intensité des efforts de recherche, de publication et de vulgarisation sont comparés à l'évolution de paradigmes sociétaux différents. Cette frénésie à tenter de trouver des compromis socialement acceptables auxquels les utilisateurs voudraient volontairement adhérer, semble viser à empêcher que « la pâte à dents ne quitte le tube » puisqu'elle offre, dans un cadre contrôlé, divers avantages répondant à des besoins exprimés par les utilisateurs, alors que d'autres solutions beaucoup plus drastiques et visant à replacer le contrôle entre les mains des utilisateurs (plutôt que des opérateurs) sont en cours d'émergence.

Tout d'abord, des efforts importants sont déployés pour porter *Tails* sur processeurs ARM. *Tails* est une distribution de Linux spécialisée dans le fait qu'elle ne laisse aucune trace

aussitôt la machine éteinte, cette propriété est dite d'« amnésie ». Diverses méthodes sont également présentées dans cette distribution pour obfusquer son fonctionnement pendant qu'elle opère. C'est avec *Tails* qu'Edward Snowden a réussi à exfiltrer nombre de documents pendant qu'il travaillait à l'intérieur même de la NSA. Le fait de porter cette technologie vers une plateforme mobile peut inquiéter divers acteurs, en particulier les autorités responsables en matière de sécurité des télécommunications puisque le résultat est un point de transmission fantôme et mobile que l'on ne peut pister par l'analyse du réseau et dont la mobilité permet d'échapper à la surveillance physique. D'autres efforts sont déployés afin de développer des téléphones qui opèrent sur plateforme x86, ce qui serait un changement majeur, assurerait une compatibilité mutuelle et, de fait, permettrait à *Tails* de rouler sur des appareils mobiles. Notons que *Tails* et surtout son composant *Tor*, font polémique.

La dernière technologie recensée dans la littérature qui sera mentionnée dans la présente (méta-)revue est *Docks* (et *Qubes*). Ces technologies reposent sur les concepts généraux de virtualisation et d'isolation au-dessus d'une couche minimaliste au niveau noyau (« *kernel* »). Ainsi, l'appareil mobile n'est qu'un point de contact et de traitement et il n'a pas vraiment conscience de ce qu'il « joue ». Toutes les considérations relatives au système d'exploitation seraient contenues dans un « conteneur » distinct. À son tour, ce conteneur serait totalement aveugle quant au contenu du conteneur « utilisateur » qu'il opère. On généralise ainsi, à au moins deux niveaux, le concept de conteneur. Cela permettrait notamment d'enregistrer l'état de la session (comme dans une machine virtuelle) et lorsque le téléphone manque de batterie, il n'y a aucun problème ni perte de données, il suffit de rebrancher et tout revient à l'état actuel exact, même plusieurs années après. Cela permettrait également de télécharger son système d'exploitation : un appareil pourrait donc, si *Apple* le permet, basculer de mode *Android* à mode *iOS*. Enfin, cela permettrait de télécharger son profil de manière temporaire. Il serait donc possible de prêter son téléphone en toute sécurité et les deux espaces seraient totalement isolés. Contrairement à *Tails*, Docker n'est pas entouré d'une aura sulfureuse, ni d'une réputation justifiée par le potentiel de danger pour lequel il semble avoir été conçu. Au contraire, Dockers semble être une initiative changeant les paradigmes de l'utilisation de l'informatique et, accessoirement ou incidemment, offrant une grande opportunité de reprendre le contrôle des données par les UFs. Notons que les efforts pour offrir Docks (ou Dockers) sur plateforme mobile sont à leurs touts premiers balbutiements.

Résumé des modèles d'affaires imputables à *Android*

On peut comprendre que les modèles d'affaires exploités par Google sont essentiellement basés sur la publicité, mais également sur les services (ex : *Google Cloud*, *Google Drive* et *GMail*, services version Premium) Cette approche (basée sur la publicité) est l'approche la plus répandue en matière de « gratuité » ou financement et elle précède Google bien que Google en soit maintenant le principal acteur, notamment avec l'achat de la compagnie AdMob, en 2009 [247]. Par ailleurs, le prix des publicités de recherche se monnaie de manière plus élevée que celle d'affichage et l'annonceur doit payer, sous Google, par clic et non par vue. Ce clic doit donc se valoir.

Par ailleurs, diverses initiatives telles Google Fiber ont vu le jour et elles présentent des offres très alléchantes. Chaque opérateur s'adapte en fonction de son public-cible et, sur un ton un peu plus exotique, *Facebook* cherche, sur la foi de ses brevets, à joindre le marché de la jeunesse des pays en voie de développement, notamment au travers du déploiement de drones offrant le WiFi dans les régions moins développées et Google demande un brevet relativement à des ballons pouvant diffuser du signal Internet (« projet *Loon* »).

Précisions concernant le « mode superutilisateur » (« *root mode* »)

Attendu qu'elle dérive de Linux, il existe, sur la plateforme *Android*, un mode « superutilisateur », (« *root mode* ») lequel n'est pas le mode dans lequel l'appareil mobile est livré par défaut. Ce mode n'est d'ailleurs pas nécessaire pour la plupart des opérations et des utilisations ordinaires, incluant le développement d'application, l'exfiltration de données, l'encryption intégrale de l'appareil et plusieurs fonctions de débogage par le port USB. Afin d'éviter que les utilisateurs ordinaires n'adoptent des comportements risqués et n'aient des ennuis avec leurs téléphones, l'accès à ce mode est plutôt complexe. Or, il ne s'agit pas d'une fonctionnalité externe condamnée par l'opérateur de la plateforme. La position de l'opérateur à cet égard n'est pas de condamner ce mode d'opération, mais de ne pas le supporter et de ne pas le recommander [356 et 357]. Contrairement à *Apple* qui a un intérêt intrinsèque en matière de DRM, la position de Google semble être basée sur des considérations de gestion des risques, en particulier avec des opérations sensibles, telles les

fonctions de GIDIM ou de paiement. À ce chapitre, Google a carrément rendu les fonctionnalités de paiement indisponibles aux appareils ayant fait l'objet d'une telle modification. Bref, Google Wallet et les services qui en dépendent sur l'appareil sont automatiquement indisponibles sur les appareils « *rooted* ». De plus, bien que l'opérateur ne condamne pas ce genre de pratiques, il cherche à s'assurer en tout temps de cet état de fait, notamment avec l'introduction d'une «e/q-fuse », un fusible logiciel (et parfois matériel) permettant à l'OP de savoir si l'appareil a fait l'objet d'une telle modification ou non. Enfin, rappelons qu'il y a certains parallèles entre l'utilisation d'un appareil *Android* sous son état « *rooted* » et celui d'un appareil *iOS* sous son état « *jailbroken* ».

Le processus par lequel on atteint ce mode requiert usuellement de reprogrammer son appareil (afin d'éviter un accès non-autorisé aux données existantes) et s'apparente à celui pour introduire une version alternative (mod) d'*Android.* Elle se fait usuellement par carte SD ou par port USB.

2.7.3 Modèle Knox

À la section [S: 1.2], il a été question des systèmes de gestion d'appareils mobiles. Ces systèmes s'inscrivent généralement dans la tentative de concilier les contradictions inhérentes de la philosophie « *Bring Your Own Device* » (« *BYOD* ») et peuvent se confronter aux défis et difficultés relatifs à la mise en œuvre et à l'application des politiques de l'entreprise sur les appareils mobiles souvent personnels. Ces systèmes peuvent ou pourraient trouver grandement utile d'avoir des points de raccordement favorables à cet effet au cœur même de l'appareil mobile, soit sa couche système. Ainsi, Samsung a fait une percée dans le segment des appareils mobiles de catégorie mi-haute et haute, avec les prix qui les accompagnent, en introduisant la technologie Samsung Knox.

Cette technologie va dans le sens des travaux de Smalley décrits plus haut et de l'utilisation de conteneurs sécurisés dans la téléphonie mobile. Ainsi, il apporte une segmentation entre divers conteneurs liés à des identités distinctes d'employés d'une même compagnie ou de compagnies différentes. De plus, il permet une segmentation entre l'utilisation personnelle et

l'utilisation d'affaires du même téléphone, avec le principal avantage que l'une ne compromet pas l'autre. Bref, il évite de traîner plus d'un appareil pour les gens aux rôles multiples.

Attendu que cette technologie est considérée comme pivot de départ, il serait pertinent de s'attarder quelque peu sur son architecture. D'une part, celle-ci est fort innovante, d'autre part, elle demeure perfectible et c'est sur le caractère perfectible que les parties ultérieures tenteront d'apporter des développements. Enfin, Knox peut aussi s'inscrire dans une perspective géopolitique faisant suite à deux révélations, la première à l'effet que les États-Unis d'Amérique aient espionné la présidente de la Corée du Sud, pays où réside le centre décisionnel et siège social de Samsung, et la seconde étant que la CIA aurait visé particulièrement des modèles populaires de divers appareils Samsung à des fins de découverte et exploitation de vulnérabilité afin de gagner un accès non-autorisé.

D'abord Samsung Knox est une initiative réservée aux appareils fabriqués par Samsung, lequel détient une part importante du marché des appareils mobiles. Cette initiative s'inscrit donc dans une perspective de gain de parts de marché, en particulier sur le segment de l'utilisation des technologies mobiles dans le cadre de fonctions d'emploi.

À cet égard, le but visé est d'éviter aux employés d'avoir à traîner deux cellulaires, un pour leur usage personnel et un pour leur usage professionnel. Ces deux usages ont des profils de risque bien distincts et leur conciliation requiert la recherche et la définition d'un équilibre délicat qui a tendance à s'avérer favorable aux prérogatives de l'employeur, ce qui est souvent d'ailleurs normal dans un contexte où c'est l'employeur qui débourse pour acheter l'appareil et qui, par conséquent, en est le légitime propriétaire, laissant l'utilisateur être un bénéficiaire de l'usufruit, à l'entière discrétion et sous le contrôle formel des politiques applicables par l'autorité patronale. Or, ce bénéfice de pouvoir utiliser une ressource dispendieuse (l'appareil mobile, souvent d'un modèle appartenant à un segment supérieur de la marque) peut s'avérer une astuce bien réfléchie permettant de rejoindre l'employé en tout temps, hors des heures, possiblement pour en solliciter, de temps à autre, son secours ou son apport ponctuel. Cela a également comme effet de déplacer une partie des activités personnelles de l'employé sous le contrôle de l'employeur, ce qui peut créer un contexte favorisant la tentation de ce dernier de tenter de « mieux connaître » son employé, en

particulier selon ses habitudes hors du travail. C'est là que les pouvoirs publics ont dressé des mesures de protection, voulues en faveur des employés. Notamment, en Allemagne, il est question du droit à la déconnection, où c'est à même les politiques déployées par les MDMs et autres utilitaires de GIDIM en entreprise que sont codifiées les empêchements formels de se connecter au réseau de l'entreprise en-dehors des heures. Au Canada, les protections concernent surtout l'expectative raisonnable de vie privée et érigent une clôture morale autour des yeux de certains employeurs trop curieux à l'égard de la sphère privée et personnelle de leurs travailleurs.

Peu importe quels seront les paramètres d'affaires, un outil comme Samsun Knox vise à permettre de déployer, auditer et surveiller diverses politiques d'entreprise sur une version quelque peu renforcée (au chapitre de la sécurité) d'*Android.*

Knox se structure donc en deux composants, soit l'application (ayant un niveau d'insertion particulier, avec des interfaces d'accès direct à la couche système) et le logiciel de gestion à installer du côté serveur, « *Samsung SDS Identity and Access Management Enterprise Mobility Management* » (SMD IAM EMM, un MDM) offert en mode compatible infonuagie. Ainsi, les fonctionnalités que Samsun Knox offre s'articulent autour de :

1) GIDIM – Authentification unifiée (SSO)
2) Isolation
3) Gestion réseau
4) Gestion centralisée

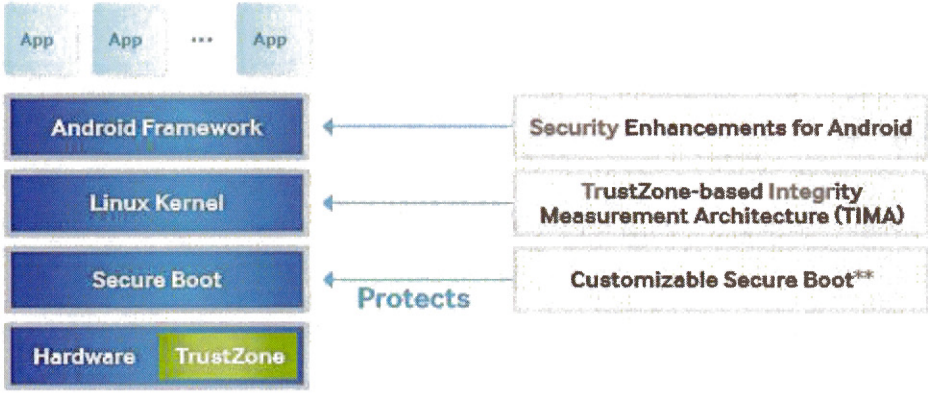


Figure 2.2 – Figure 2 du *Knox 2.0 Whitepaper*, par Samsung (2013), illustrant l'empilage de couches de protection sur laquelle se base Knox (similaire à [S : 2.3.5]).

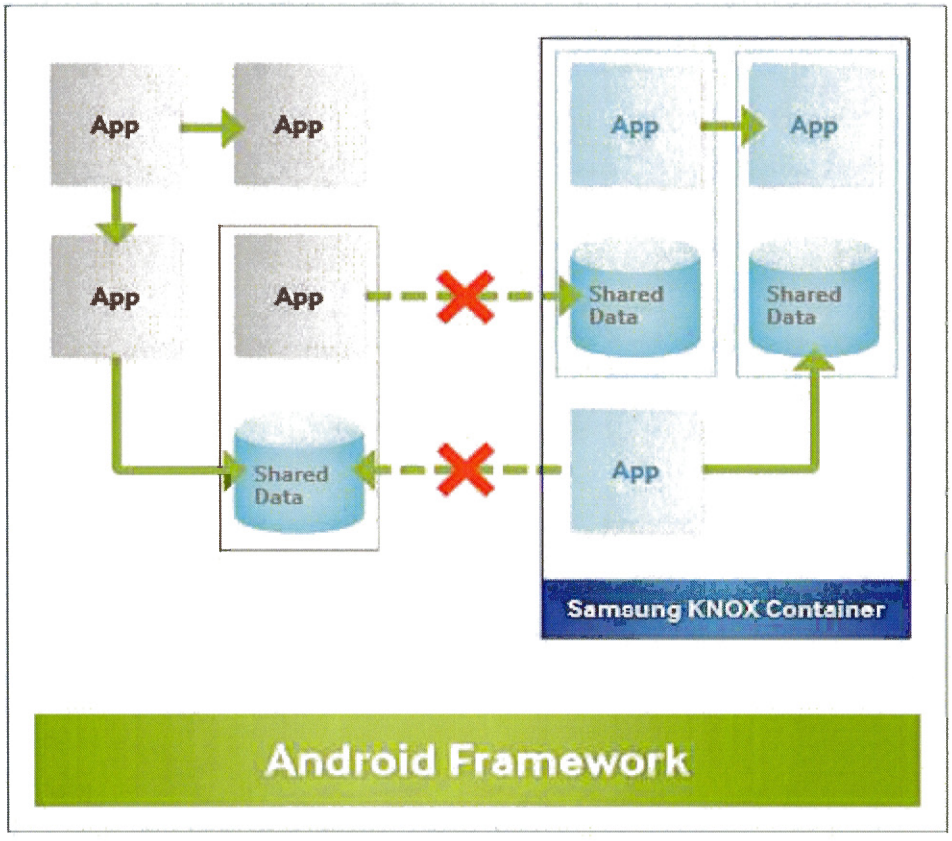


Figure 2.3 – Figure 4 du *Knox 2.0 Whitepaper*, par Samsung (2013), illustrant la stratégie de conteneurs employée.

D'abord, la pièce maîtresse de toute stratégie visant à simplifier la multiplicité des rôles est l'unification de l'authentification (SSO). Knox permet donc aux applications d'utiliser l'interface à cet effet. Dans un cadre d'entreprise, cela est fort utile puisque cela permet de s'arrimer avec les diverses autres technologies déjà en place en la matière. De manière classique, le composant serveur échange avec un service de type Active Directory (ou ses dérivés).

Ensuite, le deuxième service offert est celui d'isolation. Cela s'effectue au travers de modifications similaires à celles proposées par Smalley, soit un contrôle des accès de type MAC plutôt que DAC, ainsi que l'utilisation de contextes d'utilisation distincts matérialisés sous la forme de deux conteneurs logiciels distincts, unis uniquement par l'interface.

Puis, un ensemble d'outils permet d'effectuer la gestion réseau, notamment en ce qui concerne l'authentification et la qualité du service auprès de points d'accès (APs) sans-fil, ce qui correspond à une fonctionnalité classique des MDMs.

Enfin, en ce qui relève des outils de gestion centralisée, ceux-ci permettent l'élaboration (conception), l'expression, la mise en œuvre et le déploiement de politiques sur l'ensemble du parc d'appareils mobiles ou bien sur des segments définis selon la granularité recherchée. Cela aussi relève des fonctionnalités ordinaires des MDMs et inclut, au surplus, des outils permettant de gérer divers *scenarii*, incluant sans s'y limiter ceux de compromission (piratage) ou de vol de l'appareil mobile avec diverses ripostes, incluant habituellement la quarantaine ainsi que l'effacement à distance des données (en fait, il s'agit plus simplement et rapidement de l'effacement de la clé cryptographique permettant d'interagir avec la partition où loge le stockage du conteneur avec les données de l'entreprise, suivi d'un redémarrage afin de s'assurer de l'impossibilité de récupérer cette clé, le tout pouvant aussi couvrir, si besoin est, les données personnelles).

Knox présente donc, une série de fonctionnalités permettant de combler l'écart entre certains besoins exprimés et la configuration par défaut telle que fournie par Google. Or, cette approche a quelques déficiences :

1) Elle n'est accessible que sur les appareils Samsung
2) Elle ne répond toujours pas aux besoins des utilisateurs, mais de leurs employeurs
3) Elle n'est pas généralisable à la segmentation de tout type de profil
4) Elle comporte quelques limitations techniques qui pourraient être améliorées

Une fiche résumant les caractéristiques de la plateforme Knox sera produite aux résultats

2.7.4 Modèles de Google « *Take Out* »

Il y a eu des évolutions importantes relatives aux modèles de données au fil des ans et celles-ci peuvent se constater dans les structures de données d'archivage.

D'une part, dans *Apple*, il n'y a pas d'option officielle permettant d'exfiltrer l'ensemble des données vers un format neutre. De plus, il n'y a pas de gestionnaire des fichiers qui permette d'extraire une partie importante des données vers un autre support physique ou réseau et la conception du modèle de sécurité d'*iOS* ne prévoit pas d'espace commun pour permettre des échanges entre applications. Cependant, l'existe nombre d'outils officieux permettant d'extraire les données à partir du compte *iCloud* ou à partir des dernières sauvegardes de l'appareil mobile, si celles-ci ne sont pas cryptées.

D'autre part, du côté de Google, il existe le service *Google Take Out*. Celui-ci permet de sortir une partie importante des données d'un compte. Or, ce ne sont pas encore toutes les données emmagasinées qui sont disponibles pour emporter. Par exemple, lorsque l'on crée un fichier Google Docs, il y a plusieurs données qui sont produites et que Google détient, mais qui ne se retrouvent pas dans l'archive disponible en *Google Take Out*. Par un autre exemple, les (méta-)données de consultation d'un fichier Google Docs ou bien les modèles d'accès à ceux-ci, ou bien les nombreuses versions intermédiaires, disponibles tant que le document est en ligne, ne se trouvent pas sur Google *Take Out*. Également, les recherches peuvent se trouver, mais pas les résultats de recherche. L'historique de *Youtube* peut se trouver, mais pas toutes les donnes relatives à l'expérience de visionnement (pauses, retours, etc.), alors qu'il semble fort probable que Google les ait colligées et analysées, voire même que la compagnie en détienne encore une copie. Une autre série de question est celle des données dérivées, généralement générées par des processus d'apprentissage-machine, étant

des produits exclusifs ou partagés : comment les départager et en imputer l'origine? à qui en attribuer la propriété? à qui les communiquer, tout en respectant auto-détermination sur les données et vie privée?

Si on considère que parfois ces archives contiennent plusieurs giga-octets de données, on peut difficilement invoquer un manque de place pour justifier ces omissions. Il y a donc une motivation, qui demeure encore inconnue et à ventiler, qui justifie ces importantes omissions.

2.7.5 Autres plateformes - historiques

Très brièvement, d'autres plateformes historiques peuvent être décrites. Celles-ci ont évolué, puis sont passées à l'Histoire, laissant derrière elles des apprentissages qui peuvent être utiles à la présente activité de recherche. Les principales plateformes historiques en matière d'informatique mobile ont donc été Symbian, PalmOS, Maemo pour Nokia, et surtout, *Blackberry*.

Maemo a surtout apporté une réflexion sur la faisabilité d'opérer des appareils d'informatique mobile sous des plateformes entièrement ouvertes. À cet égard, l'initiative était vraiment orientée envers la satisfaction des besoins des utilisateurs. Notamment, cette plateforme, sous sa série N810W cherchait à offrir un service WiMax capable de concurrencer le service cellulaire via l'offre complémentaire de solutions VoIP. La plateforme était non pas basée sur un quelconque *-nix, mais une distribution de Linux connue et l'ensemble des composants logiciels étaient en code source ouvert. De plus, elle supportait plusieurs déploiements APK-Debian. Le développement de Maemo a résisté à l'achat de Nokia par Microsoft, lequel promeut surtout *Windows Mobile*.

Ensuite, *Blackberry* a connu une grande pénétration du marché [358 à 360], en particulier des segments d'affaires. La longue agonie [361 à 364] de cette compagnie peut être analysée sous l'aspect de la résistance de certains utilisateurs à changer de plateforme alors que d'autres, souvent plus jeunes, étaient en hâte de migrer vers une plateforme au fini plus léché et à la philosophie davantage orientée vers le divertissement. Bref, les deux principaux enseignements à tirer de *Blackberry* sont, d'une part, qu'il y a une importante niche

d'utilisateurs qui cherchent à utiliser leurs appareils à des fins professionnelles, avec les besoins particuliers afférants; et d'autre part, que la meilleure manière de favoriser l'adoption d'une technologie peut être de la rendre ludique et attirante.

2.7.6 Opération sous *iOS* « *jailbreak* »

Il existe une variante de la plateforme *iOS* qui doit être mentionnée, ainsi que son modèle d'opération natif, puisqu'il s'agit de la principale « extension » (apocryphe) au modèle *iOS*. Il s'agit ici des plateformes *iOS* avec modification « *jailbreak* » (libération, ou sautage, des verrous, « évasion de prison »). Il s'agit d'une modification apocryphe non-supportée en cas de soucis (restauration) par *Apple* et vivement déconseillée par celle-ci, voire illégale dans plusieurs juridictions. Cette variante se distingue du fait que plusieurs éléments de contrôle de la sécurité d'*Apple* ont été subvertis et mis hors-service. La principale motivation derrière l'adoption de ces versions est le désir des utilisateurs d'avoir le contrôle sur leur appareil, de se soustraire au contrôle d'*Apple* sur ce dernier et, notamment, de pouvoir installer des applications (augmenter leur capacité applicative) au-delà de ce qu'*Apple* permet. Par exemple, il est nécessaire d'avoir un tel accès pour disposer de la capacité d'installer des applications donnant accès à du contenu non-payant (libre de droits ou, le plus souvent, pirate) tels des flux vidéo (Pirate *Apple* TV, « *PopCorn Time* », etc.), pour exercer un contrôle plus avancé sur le réseau WiFi ainsi que sur des fonctionnalités de récupération de fichiers (« *Undelete* ») et de gestion des albums photos hors des infrastructures applicatives fournies par *Apple*. Notons que le principal risque, outre les mesures de rétorsion d'*Apple*, est l'exposition à des codes exécutables malveillants ainsi que la perte des données de GIDIM [425]

2.7.7 Résumé des différences entre les plateformes *Apple* et *Android*

Au risque de se répéter, il est pertinent de colliger brièvement les principales différences entre les plateformes *Android* et *iOS*. Prime à bord, celles-ci sont philosophiques, c'est-à-dire que, bien que toutes deux partent d'un noyau basé sur Unix, la conception, le type d'utilisation et même l'idéologie diffèrent de manière considérable entre les deux. Tout d'abord, *iOS* est propriétaire alors que *Android* est plus ouvert. Cela limite grandement les développements que l'on peut apporter au cœur même de la plateforme, essentiellement de l'absence

d'implication de la communauté et surtout, des programmeurs bénévoles. Cela écarte aussi la possibilité de voir prospérer légalement des versions dérivées ou alternatives. Ensuite, *iOS* favorise les restrictions du contrôle que l'UF pourrait avoir sur le contenu, notamment à cause de l'importance des stratégies DRM chez *Apple*. En ce qui concerne la GIDIM dans son sens classique et strict, *Apple* opère un contrôle centralisé et exclusif alors que Google opère un contrôle techniquement fédéré (avec *OAuth*), mais *de facto*, centralisé. En ce qui concerne les données, *Apple* et Google les collectent tant l'un que l'autre, mais leur attitude correspond à leurs modèles d'affaires respectifs. Le modèle d'*Apple* se base principalement sur la consommation payante (*iTunes*) alors que celui de Google principalement sur la consommation « gratuite » (*Youtube*). De ces faits, *iOS* ne permet pas d'exporter facilement ses données par des outils connus puisque *Apple* n'a pas intérêt de laisser un client partir. De son côté, Google, bien qu'il offre un accès à une grande part de ses propres données via l'outil *TakeOut*, ne permet pas d'extraire la totalité des données, directes ou dérivées. Google garde jalousement les données traitées (ex : les associations ou inférences) ainsi que certaines données brutes. Enfin, *Apple* interdit formellement toute altération à son produit alors que Google ne le recommande pas, sans toutefois l'interdire, ce qui semble correspondre à sa tendance globale de permettre un meilleur contrôle sur une plus grande partie des actifs informationnels des UFs.

2.7.8 Autres plateformes – actuelles

Il existe, par ailleurs, d'autres plateformes actuelles que celles présentées. Celles-ci ne seront présentées que très brièvement puisque leur adoption est marginale et que peu d'indices ne laissent présager une explosion de leur croissance (à une exception près). Toutefois, l'obligation éthique de transparence dans la recherche requiert de les mentionner. La principale version qui gagne en popularité, tout en demeurant marginale, est « *Tizen* », un nouveau système d'exploitation, basé sur Linux et développé principalement par Samsung afin de s'assurer, en qualité de premier fabricant d'appareils mobiles, une certaine indépendance par rapport à Google. En absence d'une infrastructure de GIDIM aussi évoluée que celle de Google, l'approche adoptée, au moment actuel, est basée sur une stratégie de sécurité contenue dans l'appareil plutôt que basée sur la connectivité [369]. Tizen regroupe la fusion d'autres projets dont Bada.

Avant Tizen, l'initiative la plus prometteuse était celle de l' « *Ubuntu Phone/Touch* », laquelle fut interrompue en avril 2017, ce qui laisse penser que les difficultés techniques rencontrées (gourmandise en ressources processeur et mémoire vive) ainsi que l'acquisition de *Canonical* (l'entreprise derrière la coordination d'Ubuntu) par Microsoft ne sont peut-être pas étrangères à cette décision. Ensuite, il y a Firefox OS et Chrome OS, toutes deux des initiatives basées sur l'utilisation de HTML5 comme langage fondamental de développement au-dessus d'une mince couche système en C++, C et assembleur. Chrome OS base sa GIDIM sur des stratégies fédérées autour de *OAuth*, tout comme comptait le faire Ubuntu/Touch. Ensuite, il y a « *Windows Mobile* », lequel base sa stratégie de GIDIM sur les modèles indirects « *CardSpace* » [366] (identité en tant que service tiers, maintenant renommé « *Microsoft Access and Identity Solutions* » [365] et adapté à l'infonuagie).

Puis, le dernier et non le moindre parmi les produits tout-public est l'arbre de l'ensemble de versions « *Sailfish OS* » / « *MeeGo* » / *Mer*. Celles-ci sont issues du développement continu mené par Nokia à la suite de Maemo. D'un point de vue architectural, on y trouve les principaux concepts et considérations philosophiques identifiés, dans la littérature, au courant de la présente étude. À plusieurs égards, cette plateforme et son développement sont innovants, voire révolutionnaires. Par exemple, le leadership de développement est mené par la communauté sous une formule de méritocratie [368] formalisée, l'architecture du système est intégralement modulaire et le contrôle des accès par défaut est sous la forme « contrôle d'accès obligatoire ». La GIDIM est fédérée et le moteur de GIDIM est à même chaque appareil. Donc, un appareil peut servir à identifier des réseaux d'appareils. Malgré toutes ces innovations, l'Histoire récente [367] nous apprend que la supériorité technologique n'est pas automatiquement un gage d'adoption.

Enfin, il ne faut pas oublier qu'il existe des plateformes spécialisées, telles Tails Mobile, visant spécifiquement à couvrir les segments du marché des utilisateurs qui ne veulent laisser absolument aucune trace.

2.7.9 Modèles de GIDIM existants

Les principaux modèles de GIDIM sont des modèles exclusifs et fixes, c'est-à-dire que le modèle est intrinsèque et que c'est la seule option disponible, bâti à même la plateforme et ne peut être changé Cela contraste avec les modèles modulaires où celui-ci peut être changé. Ensuite, la plupart des modèles sont utilisés en mono-session, c'est-à-dire qu'un seul utilisateur peut utiliser l'appareil à la fois, même s'il y a plusieurs instances ou « sandboxes » en même temps. Puis, ils ne sont certes pas obligatoires, mais leur non-utilisation résulte en une limitation importante des capacités applicatives des appareils. Ensuite, bien qu'*Android* utilise théoriquement une technologie de GIDIM fédérée, dans les faits, il s'agit d'une technologie de GIDIM centralisée. Dans les deux cas, la plateforme offre une capacité de GIDIM intégrée, permettant à chaque application d'utiliser les services de GIDIM du système, mais la plupart des éditeurs d'applications ont choisi de ne pas intégrer pleinement ces fonctionnalités : les applications lisent les infos de GIDIM disponibles, mais se basent sur leurs propres systèmes de GIDIM, ce qui accroît la charge cognitive [370 à 374 et 426] et le risque de divulgation. Ensuite, dans les faits, *Android* permet la pluralité des utilisateurs (GIDIM autorisant la concurrence, asynchrone, par contre), mais cette option n'est pas très utilisée. Dans le même ordre d'idées, *Android* présente théoriquement deux modes d'opération (celui du superutilisateur et celui de l'utilisateur), mais dans les faits, seul le dernier est utilisé dans la plupart des cas. Enfin, il n'existe pas de modes opératoires en matière de GIDIM, ni dans l'une, ni dans l'autre des principales plateformes. Il existe, au niveau applicatif, parfois un mode opératoire alternatif (ex : « (Mode) Onglets *incognito* » dans Chrome), mais cela n'offre pas les mêmes garanties que si la même option était offerte comme enchâssée au niveau système.

Tableau 2.2 – Synthèse des déficits actuels constatés en matière de GIDIM

Unix						Windows
Apple		*Android*				Autres
Ordinaire	*Jailbreak*	Ordinaire		Mods		
		N-Rooted	*Rooted*	*N-rooted*	*Rooted*	
Centralisation Inflexibilité Monolithicité	Fiabilité (manque de …)	Centralisation Vie privée Abus position dominante	Centralisation par défaut Abus position dominante Monomodicité	Variable Abus position dominante	À déterminer	Vie privée Centralisation

2.8 Déficits constatés

La présente section met en lumière les déficits des différents modèles de GIDIM actuels, tantôt d'un point de vue opérationnel, tantôt d'un point de vue politique et tantôt d'un point de vue technique. Elle recense donc ce qui constitue l'écart entre les besoins identifiés et la situation actuelle.

2.8.1 Inadéquation des modèles de GIDIM – discussion générale

D'abord, d'un point de vue général, la principale inquiétude est la jonction du caractère constant de la collecte de renseignements personnels qui s'opère et du fait que cette collecte continue soit associée à une identité. Ce lien transforme dans les faits des données personnelles en des données de GIDIM. Par exemple, le fait que l'on se connecte depuis un nouvel endroit géographique (un autre pays) peut déclencher des mesures de vérification du côté du fournisseur de GIDIM et requérir pour l'utilisateur de se soumettre à des routines de vérification de sécurité (ex : question de sécurité). En soi, ce n'est pas la surveillance qui dérange, c'est la totale absence d'exclusions et de contrôle de la part des utilisateurs qui semble déranger. Cela donne une impression pouvant être allégoriquement représentée sous

forme d'œil, sans paupière, qui surveille depuis le ciel, sans répit, et qui ne laisse aucun espace d'angle mort; cela revêt une dimension assez proche de ce qui rebute plusieurs individus dans le discours religieux classique et moral. En soi, le caractère faillible des individus a comme conséquence inéluctable dans ce contexte que, sur la durée, surtout si on multiplie les lois qui codifient en infraction divers comportements répandus, mais considérés comme indésirables, chacun sera immanquablement pris sur le fait, tôt ou tard. À ce stade, chaque citoyen sera vulnérable à la compromission et au chantage, dans la plus stricte et rigoureuse légalité.

Ensuite, il y a un problème dans l'absence de liberté et de véritable choix en matière de fournisseurs de services d'identité et dans leurs processus. Enfin, il y a toute la dimension relative à la souveraineté et au contrôle par les UFs sur leurs données qui semble les perturber. Ainsi, les technologies mobiles sont certes des outils, mais encore faut-il se demander au service de qui sont ces outils.

2.8.2 Considérations politiques dans les critiques en matière de la GIDIM actuelle

On attribue [375] au Cardinal Richelieu (ou parfois au magistrat Laubardemont ou au bourreau Laffémas) : « Qu'on me donne six lignes écrites de la main du plus honnête homme, j'y trouverai de quoi le faire pendre. » Cela illustre le cœur de la problématique : il y a un malaise à ce qu'il y ait un outil pour colliger systématiquement nos turpitudes, certaines pouvant être assez graves. Une situation où, en fouillant un peu, on peut obtenir suffisamment d'éléments compromettants pour faire condamner ou chanter qui on veut n'est pas compatible avec une société libre et démocratique. Dans un monde sans pardon ni oubli [376], la saga Ahsley Madisson [377] rappelle à tous et chacun que notre passé numérique est un fantôme éternel.

Le premier palier de risque est la découverte inopinée par quelqu'un que l'on connaît, par exemple, la douce moitié ou les enfants. Ce risque peut être mitigé en effaçant systématiquement ses traces. Notons cependant que ces comportements que l'on désire cacher ne sont pas nécessairement répréhensibles et qu'il y a une question éthique qui émerge

de la situation actuelle : la transparence totale est-elle éthiquement souhaitable? Notons que ce tiers connu n'est pas nécessairement une personne physique, tel un membre de la famille, mais peut aussi être un employeur. Ensuite, il y a le risque que les opérateurs de plateforme ou d'applications connaissent des renseignements compromettants sur nous, ou bien qu'ils connaissent tellement de renseignements que l'utilisateur s'en trouve affaibli dans son rapport avec l'opérateur, par exemple, s'il devenait désespérément prévisible. Ce risque ne se limite pas aux opérateurs de plateforme, mais s'étend également à tous les partenaires avec qui ceux-ci peuvent partager des renseignements. À cet égard, la meilleure protection provient probablement d'une législation d'ordre public de protection efficace combinée à un pouvoir décisionnel effectif qui permette que les contrats liés représentent vraiment un consentement libre et éclairé; voilà des objectifs à l'égard desquels il semble encore y avoir une distance considérable. Ensuite, vient le risque que l'État, local ou étranger, désire prendre des mesures qui auraient des effets sur les UFs, possiblement à leur défaveur, sur la base de données produites par eux-mêmes. Cela viendrait en collision frontale avec les principes de protection contre les fouilles abusives et l'autoincrimination. À l'encontre de ces risques, la protection doit venir en partie de l'État (par ses garanties constitutionnelles), en partie des individus (par leur comportement prudent), en partie des OPs (par la mise à disposition de solutions technologiques) et en partie par des technologies connexes. Les considérations relatives à ce dernier risque sont particulièrement sensibles parce qu'une protection trop grande des secrets pourrait empêcher les États d'exercer leurs fonctions régaliennes, dont celles de protection, mais une protection trop faible mine les idéaux de liberté et de démocratie qui justifient l'État même. Ce qui complique la tâche en plus, c'est le fait que plusieurs glissements ont mené à se demander si les contrepoids, tels ceux du contrôle judiciaire, sont encore efficaces pour assurer les protections requises. Enfin, il y a le risque principal d'être la cible de piratage en tant qu'activité économique criminelle organisée, lequel dépend de la notoriété de l'individu et de la valeur de ses actifs informationnels, selon un cadre ou un autre. À cet égard, il y a un risqué ciblé relatif à la capacité d'agrégation, propres aux réseaux d'information d'authentification faiblement protégés où les réponses aux questions de sécurité des uns sont disponibles aux autres.

2.8.3 Considérations techniques dans les critiques en matière de la GIDIM actuelle

Même en absence de toute considération morale, éthique ou politique, les stratégies de GIDIM actuelle présentent des déficits sur plusieurs fronts techniques. Notamment, au niveau de l'ergonomie, l'incapacité de déléguer une identité à un appareil connecté constitue un exemple de limitation qui pourrait être facilement corrigée. De plus, la duplicité des profils que tentent de gérer des solutions de type MDM illustrent qu'il y a des déficits dans la conception, au niveau de la plateforme, des principales offres en matière d'informatique mobile. Ensuite, les processus de GIDIM sont quelque peu désuets et trop sommaires. Par exemple, ils n'offrent pas la possibilité de déléguer à un tiers de confiance la possibilité de recouvrir une identité compromise (ou de départager des assertions inconciliables d'aspirants à la même identité), ni de planifier son héritage numérique, ni de prendre en compte la perte de certaines facultés (telles la mémoire ou la voix) sollicités par le processus de GIDIM, mais qui se détériorent au fur et à mesure que survient le vieillissement chez l'individu. Enfin il n'y a pas vraiment de front uni qui semble offrir des caractéristiques techniques ou opérationnelles nécessaires à convaincre les opérateurs de plateformes ou d'applications d'unifier et d'intégrer leur stratégies de GIDIM, ce qui mène à nombre de dédoublements. Cette liste des inadéquations techniques en matière des stratégies de GIDIM actuelles n'est toutefois pas exhaustive.

CHAPITRE III

MÉTHODOLOGIE

La méthodologie retenue est celle de l'analyse documentaire, sous ses formes descriptive et comparative en vue de produire un modèle. Dans le cas d'espèce, elle s'apparente à une ethnographie puisqu'elle fait état des considérations qui se dégagent de l'étude d'une communauté ou population. Il subsiste deux limitations à ce caractère ethnographique. D'abord, la quantité documentaire spécifique au Québec n'est pas suffisante pour mener l'étude. Ensuite, les préoccupations, outre la langue, s'avèrent assez comparables (selon les éléments recueillis dans les sources primaires, telles les transcriptions des comparutions à la Commission Chamberland, la législation et la jurisprudence) à celles que l'ont trouve dans la littérature plus générale. Par ailleurs, quant à cette démarche, il s'agit d'une méthode constructiviste qui se trouvera formalisée dans la présente section.

En soi, la plupart des méthodologies [381] décrivent ordinairement plusieurs grandes familles d'étapes : la conception de l'étude, la comparaison de méthodologies et la sélection de l'une d'elles, la collecte de données, l'interprétation des données et l'élaboration d'artéfacts à partir de ces données ou de leur interprétation. En l'espèce, quant au « Comment ? »; la conception de l'étude a été abordée précédemment puisqu'il s'agit d'une méthode à la fois exploratoire et interdisciplinaire. Ensuite, quant au « quoi ? », il fut résolu de se concentrer sur l'illustration des modes d'opération sous *Android* et *iOS* ainsi que sur l'élaboration de nouveaux modes à proposer, en tant qu'évolution post-Knox. Le corolaire est qu'il ne serait pas question d'un travail d'expérimentation (ce qui fut tenté dans les versions précédentes), mais bien d'un travail qui prend la recherche documentaire et observationnelle comme point de départ. Ainsi, la méthode de recherche démarre par l'étude des plateformes actuelles et de leurs modes d'opération au travers de l'observation structurée, puis suivent des étapes d'élaboration et de rattachement de nouveaux modes d'opération à des modèles d'affaires, puis enfin, suivent des étapes d'analyse approfondie de ces modes.

Attendu que l'extrant désiré est un modèle de modes opératoires que les utilisateurs pourront utiliser pour gérer leur identité mobile, la méthodologie est l'ensemble des préceptes qui guident l'élaboration de ce modèle. Le processus est initialement décrit à la [S: Figure 1.2] de la section [S: 1.2].

En somme, il s'agit d'un cycle d'itérations incrémentales qui visent à intégrer des valeurs attribuées à des groupes ou des profils d'utilisateurs, par faisceaux, dont l'intégration doit respecter au moins un des modèles d'affaires en place pour assurer un certain réalisme.

Attendu que la revue de la littérature a déjà couvert les éléments antécédents de la démarche, la méthodologie se divise dans les étapes suivantes (et leurs sous-sections correspondantes) :

1) Éliciter les enjeux pertinents au sein de la population à l'étude en général. Une grille d'analyse doit être conçue sur la base de ces enjeux.

2) Observer et décrire les deux principales plateformes natives sur la base de la grille d'analyse mentionnée au premier point.

3) Étude des extensions et adaptation existantes

4) Élaboration des modes opératoires proposés

5) Rattachement des modes opératoires aux modèles d'affaires et aux rôles

6) Comparaison des modes opératoires

7) Identification des extensions dérivées à mettre en œuvre dérivées des modes opératoires les plus pertinents.

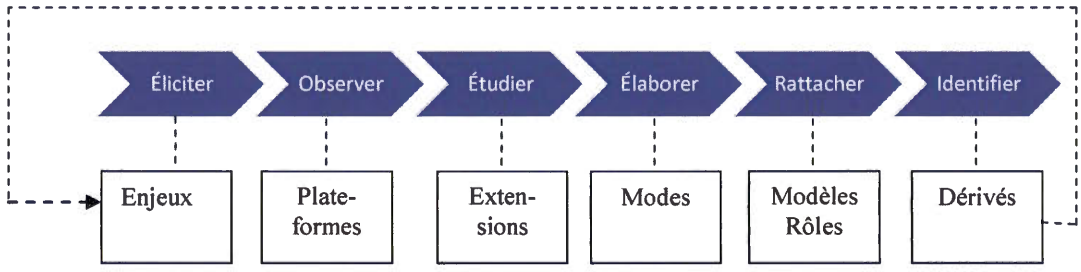


Figure 3.1 – Séquence au sein de chaque itération

Il faut répéter pour chaque enjeu, de manière à déterminer la position à prendre pour chacun et à classer chaque besoin qui en découle, soit sur une fonctionnalité existante, soit sur une extension à ajouter.

La section portant sur la méthodologie vise, entre autres, à assurer la reproductibilité des résultats de l'étude. Elle vise aussi à les rendre comparables et intégrables. En l'espèce, la grille d'analyse est un résultat intermédiaire. Un autre résultat intermédiaire est la liste des données personnelles qui sont en jeu.

Les résultats intermédiaires, s'ils divergent d'une étude à l'autre, peuvent rendre le reste de l'étude non-comparable. Cela est cependant nécessaire à permettre le maintien d'un cadre de comparabilité des démarches dans le temps ou sous toute autre dimension susceptible à induire des variations importantes. Par exemple, si les valeurs identifiées ou les renseignements collectés varient d'une étude à une autre, cela peut être dû aux changements de mœurs ou d'autres changements sociologiques ou technologiques. Dans une variation prévisible au regard de l'évolution des technologies de contrats intelligents [382] et de l'Internet des Objets, il se peut que la valeur financiarisée des opérations soit un renseignement collecté d'ici cinq (5) ans, et que la valeur financière de ces informations soit un enjeu qui se trouvera alors dans une grille d'évaluation des plateformes, toujours dans ce même horizon. Ainsi, les outils dégagés en tant que résultat intermédiaire peuvent changer, mais le processus par lequel on arrive à les élaborer demeure le même, favorisant, dans la durée, la comparabilité de l'étude.

La méthodologie doit décrire et étudier les méthodes employées au cours de l'activité de recherche, s'assurer que celles-ci soient compatibles avec l'activité scientifique et qu'elles dégagent de la connaissance valable. Cette compatibilité se fait par le respect de préceptes de rationalité, de documentation, d'intelligibilité, de cohérence et de support des données d'observation au positionnement face à des hypothèses [25]. La valeur scientifique se dégage de la capacité analytique, explicative ou prédictive, au vu des résultats, obtensible à partir des modèles et raisonnements retenus [384]. En l'espèce, il s'agit d'élaborer un modèle de modes opératoires à partir de la littérature existante. C'est donc le caractère documenté et intelligible, via une description détaillée de la démarche (voir section [S: 3.1.5]), ainsi que le

support des données d'observation (documentaire) vers les modèles proposés qui visent à garantir la validité de la présente activité. D'autre part, c'est l'utilité analytique des modèles, au regard des besoins identifiés, qui vise à donner de la valeur à la présente recherche.

Les étapes proposées visent à apporter des clarifications quant aux méthodes employées dans la présente étude. La première sous-section englobe la plupart des éléments que l'on retrouve classiquement dans tout travail de recherche et qui pourraient constituer la fiche identitaire de la méthodologie employée. Les autres sous-sections explicitent le processus intellectuel afin de répondre aux exigences de reproductibilité et d'intelligibilité de l'étude.

En soi, rien n'exclut de développer sa propre méthodologie, tant que celle-ci demeure valide au regard de ce qui rend une méthodologie valable sur le plan scientifique, tel que décrit plus haut. En fait, le développement de nouveaux outils méthodologiques est très courant puisque souvent nécessaire; au fur et à mesure que le territoire sondé avance, de nouveaux outils peuvent être nécessaires pour organiser les connaissances et les étudier de manière systématisée et rigoureuse. En ce qui concerne la version actuelle de ce document, il a plutôt été retenu de se baser sur des méthodes établies et éprouvées afin de favoriser la confection d'un artéfact succinct. Ensuite, c'est la révision par les pairs qui permet la reconnaissance ou non des outils méthodologiques ainsi développés. Notons cependant que les méthodologies sont souvent fortement indépendantes des réalités observées et que, par exemple, un outil méthodologique provenant d'une autre discipline, telle la médecine ou la criminologie, pourrait, s'il respecte certains critères énoncés plus haut, être repris dans un travail tel celui de la présente étude.

En l'espèce, au surplus des notions de méthodologie acquises au fil des cours du programme et par la lecture d'ouvrages généraux sur la méthodologie en génie logiciel, les fondements méthodologiques de la présente étude ont été puisés dans quelques ouvrages et articles :

1) *Content Analysis: An Introduction to Its Methodology* [417] monographie par Klaus Krippendorff. Celle-ci a surtout été utile pour tout le volet sur l'analyse documentaire.

2) Manuel des cours de méthodologie MIG9100 et MIG9250 [418], par Martin L. Cloutier, celui-ci a surtout été utile pour la section portant sur les éléments méthodologiques.

3) *Grounded Theory Methodology – An Overview* [419], article par Strauss et Corbin, sur la méthode « *Grounded Methodology* », essentiellement visant une méthode rigoureuse d'analyse de contenu en sciences sociales.

4) *A methodology for common-sense model development* [420] un article par M. Dohnal, paru dans le domaine de la chimie et concernant des modélisations, duquel certains préceptes en matière d'élaboration de modèles ont été retenus.

5) *Tropos: An Agent-Oriented Software Development Methodology* [421], un article par Bresciani et al., dont des préceptes en matière d'inclusion d'exigences à des modélisations existantes sont les principaux apports à la présente étude.

6) *The Conical Methodology and the evolution of simulation model development* [422] un article par Nance portant sur des modélisations dans un cadre plus formalisé et propre aux simulations, mais desquels quelques principes méthodologiques fondamentaux (propriétés, méthode d'attribution, définition, flux, etc.) en matière de modélisation ont été retenu.

7) *COMO: a UML-based component development methodology* [423], un article avant-gardiste en son temps, par Lee, Yang & al., dont la section [S: 2.4.1] a guidé le processus d'analyse et d'attribution des modèles.

8) *A Business Model (BM) Development Methodology in Ubiquitous Computing Environments* [424], un article par Leem & al., qui a été retenu puisqu'il visait déjà des modèles d'affaires dans un cadre similaire aux technologies présentement offertes par les OPs et dont l'ubiquité est un composant important. Le raisonnement de cet article a été repris en séquence de travail inversée afin d'étudier la compatibilité de divers modèles d'affaires (dans un contexte d'ubiquité, ou non) avec les modes opératoires proposés.

Bref, les documents mentionnés plus haut permettent au lecteur d'avoir une idée sommaire des origines des processus intellectuels permettant de mener l'évaluation multivariée entre les modèles d'affaires et les modes opératoires. Sur une ligne appelant à la prudence, notons enfin que, d'emblée, l'adoption d'une méthodologie d'analyse documentaire et de développement de modèles comporte des risques méthodologiques importants. À cela se rajoute le caractère qualitatif et exploratoire de la présente étude, lesquels posent des défis

supplémentaires. Notons d'abord qu'une analyse exploratoire est souvent inhéremment descriptive et qualitative.

En soi, elle jette les bases sur lesquelles des études ultérieures pourront se poser et étendre, peut-être quantitativement cette fois, le domaine de la connaissance recensée. Il faut donc commencer quelque part et c'est là, la particularité de l'étude exploratoire. Il est donc admis que la connaissance dégagée est perfectible et il est important de la communiquer comme telle, elle n'est pas exhaustive ; cela ne la rend pourtant pas invalide. Par exemple, dans le cas actuel, des études ultérieures pourraient viser à mesurer le succès des divers modes d'opération proposés, ils pourraient prendre les résultats actuels comme hypothèses de départ et induire des itérations supplémentaires

En ce qui concerne l'élaboration de modèles, c'est essentiellement le caractère multiple, libre, voire arbitraire, des modèles retenus parmi l'ensemble des modèles possibles qu'il faut surveiller. Notons d'abord qu'il eût été possible d'adopter d'autres approches qui mettent de l'avant des composants plus formels (ex : l'étude détaillée de la valorisation des données personnelles selon Parkes [384]), mais ces études très formalisées d'aspects ponctuels ne permettaient pas de dégager une vue d'ensemble qui demeure aussi rigoureuse pour le phénomène macroscopique de la GIDIM. Cette difficulté d'avoir un fil conducteur aussi solide qui transcende l'ensemble des aspects ponctuels peut indiquer que le phénomène observé est difficilement réductible (trop complexe, surtout de par ses composants ou aspects humains et sociaux) au formalisme, ou bien que plusieurs autres études sont nécessaires à bien sonder formellement le phénomène. Notons que les circonstances d'époque contraignent à faire de l'évolution des deux principales plateformes le fil conducteur de la présente étude.

Pour chacun des risques mentionnés précédemment, il y a une mesure de mitigation adéquate. Par exemple, concernant les risques de faiblesses liées au choix de l'analyse documentaire, celles-ci sont mitigées en se référant précisément à une méthode établie, en circonscrivant de manière très précise le sujet de recherche (ce qui restreint l'espace possible des digressions) et en limitant les caractéristiques de ce que l'on peut chercher, en l'espèce, des besoins à intégrer dans une démarche de génie logiciel. En ce qui concerne le caractère

exploratoire, c'est la définition précise de la portée et des hypothèses qui permet de situer la présente étude à son juste endroit et d'évaluer les connaissances qui s'en dégagent, à leur juste valeur. Enfin, concernant les degrés de libertés qui pourraient émaner de l'activité d'élaboration de modèles, c'est le fait de prendre comme point de départ des modèles existants qui permet, de pair avec le caractère exploratoire bien déclaré de la démarche, de s'assurer que le lecteur comprend que ces modèles sont proposés comme émanant d'un processus analytique et qu'ils demeurent à être mesurés et validés par des études subséquentes.

3.1 Éléments méthodologiques

La présente section fournit l'essentiel des éléments méthodologiques que l'on retrouve classiquement dans une étude similaire dans le domaine de l'informatique de gestion, tel qu'appris dans les cours MIG 9100 et MIG 9250.

3.1.1 Hypothèses

L'hypothèse principale de travail est à l'effet qu'il existe, dans la littérature, des éléments identifiables permettant d'améliorer les modes opératoires actuels en matière de GIDIM tels qu'observés, tout en étant compatibles avec les modèles d'affaires actuels. Si cette hypothèse est mal évaluée (ce qui ne veut pas dire infirmée), sous l'un ou l'autre de ses aspects, une partie importante de la présente étude est compromise. Il faut donc que les résultats permettent de valider si ces éléments identifiables existent dans la littérature; si ceux-ci, le cas échéant, peuvent améliorer les modes opératoires et enfin, toujours le cas échéant, si ces améliorations sont compatibles avec les modèles d'affaires actuels.

De nombreuses autres hypothèses, pouvant s'organiser en des réseaux complexes, pourraient être mentionnées puisqu'elles seront, à un moment ou un autre, mises de l'avant au sein de la présente étude. Par exemple, une telle hypothèse peut être à l'effet que les utilisateurs recherchent de vivre dans une société libre et démocratique ou bien qu'il existe un point

d'équilibre entre la sécurité et la liberté, mais que celui-ci est individuel, personnel et subjectif. Une mouture précédente de la présente étude faisait un recensement structuré des principales hypothèses, mais cet élément a été retiré afin de faciliter la fluidité de l'artéfact. Il n'en demeure pas moins que ces réseaux complexes d'hypothèses peuvent être utilisés ultérieurement dans d'autres avenues, par exemple, l'analyse formelle des exigences émanant des modes d'opération identifiés, etc.

3.1.2 Question de recherche

La question de recherche est normalement remplacée par l'hypothèse principale de travail qui agit, pour la suite, comme fil conducteur de l'activité de recherche [25 et 383]. En l'espèce, la question de recherche pourrait être formulée ainsi : « Par quels modes opératoires autres que ceux existant (principalement dans *iOS* et *Android*), peut-on améliorer la GIDIM? ». Tout comme pour les hypothèses, il y a une multitude de questions dans l'élaboration et la conduite de la présente activité de recherche et, ainsi, il est possible de les organiser dans des réseaux complexes pouvant être utiles dans d'autres cadres.

3.1.3 Méthodes d'acquisition de données

La méthode d'acquisition de données est essentiellement documentaire, avec une attention particulière aux commissions spécialisées sur le sujet, en général, et celles du Québec en particulier. Il y a un respect de préceptes de classement et catégorisation des éléments documentaires pris en intrant, principalement sur la base des dimensions de la qualité de l'information contenue et du traitement possible de celle-ci. Le haut du pavé, à cet égard, est réservé à la littérature académique et scientifique, suivie de la littérature technique (avec priorité pour celle révisée par les pairs), puis aux documents d'autorité gouvernementale (législation, jurisprudence), suivi des documents commerciaux (concernant leur contenu technique) et, en queue de liste, les autres sources documentaires moins formelles, incluant *Youtube*, le contenu politique et militant, etc.

Également, une autre méthode d'acquisition de données retenue est l'observation directe. Il est ici question d'observer directement, par exemple, les modes d'opération par défaut des diverses plateformes ou bien d'observer, par un processus d'informatique judiciaire, quelles données de GIDIM sont contenues ou communiquées dans l'une ou l'autre des plateformes.

Les enjeux ([S: 4.1]) sont ainsi récupérés à même la littérature étendue (incluant notamment la législation) qui est une source principale à cet effet, Idem pour les besoins et leurs métriques.

3.1.4 Méthodes d'analyse

En ce qui concerne la méthode d'analyse, elle se résume aux sept étapes mentionnées au début de la section [S: 3], et dont le détail se trouve dans ses autres sous-sections. Essentiellement, le travail d'analyse consiste en l'analyse systématisée du contenu permettant de dégager des valeurs, en l'analyse des caractéristiques des modes opératoires actuels (essentiellement le mode natif *iOS*, le mode natif *Android*, le mode proposé par Samsung Knox) et l'élaboration de nouveaux modèles, le tout mis en relation avec les modèles d'affaires actuels. C'est ainsi que se dégagent les grilles d'analyse [S :4.2], en particulier celles permettant de profiler la clientèle [S: 4.2.3] et les constats de couverture [S: 4.2.5] ou de déficit ([S: 4.2.6]) ainsi que de repérer les tendances dans les évolutions possibles [S: 4.2.7 et S: 4.2.8]. S'en suis la synthèse des modes d'opération. L'élaboration de la pensée des modes d'opérations ainsi que des modes eux-mêmes est une activité foncièrement basée sur la synthèse. Les grilles d'identification des données résidantes et communiquées ([S: 4.2.1] et [S: 4.2.2]) sont, quant à elles, dérivées d'une combinaison de processus analytique (afin de choisir les données à cibler) et d'opérations d'observation (judiciaire, « *forensic* ») avec les outils Sekomon, *FTK*, *Encase* (Mobile) ainsi qu'avec le serveur Apache utilisé en tant que *forensic proxy*.

3.1.5 Séquence de travail (*a posteriori*) de la revue de la littérature

La présente section vise à détailler le segment du fil conducteur, le parcours intellectuel de la présente étude, subséquent à la première passe de revue de la littérature. Il inclut les conclusions intermédiaires qui ont été élaborées ainsi que la synthèse des divers éléments de la revue de la littérature. Cette section vise à assurer l'intelligibilité du processus et la reproductibilité relative de la méthode. Essentiellement les sources primaires ou secondaires de meilleure qualité permettant de dégager les enjeux en matière de GIDIM tels qu'exprimés dans la population sont : la législation, les commissions parlementaires ou publiques, les initiatives gouvernementales, paragouvernementales ou supranationales (comme *REISearch*), la littérature scientifique, etc. Les sources documentaires décrivant le mieux la situation actuelle sont les cadres contractuels applicables aux utilisateurs ainsi qu'aux développeurs d'applications et la littérature scientifique. Des études, dont les détaillent suivent, sur le sujet nous informent que les utilisateurs sont peu informés de ces conditions et qu'ils se sentent impuissants à leur égard, que dans les faits, l'insatisfaction envers celles-ci s'opère davantage par des pratiques telles l'utilisation de pseudonymes que par le militantisme ou la litigation.

Ensuite, les statistiques sur la jurisprudence procurent une perspective réaliste de la facilité et de la probabilité avec laquelle l'État réussit à obtenir les autorisations judiciaires permettant d'accéder aux données privées des individus. En réaction à cela, les statistiques [385, 386 et 415] sur l'adoption de technologies de protection de la GIDIM telles Orbot ou TOR permettent de percevoir une fracture qui s'élargit. Les communications officielles [387, 389 et 391] relèvent que les États s'inquiètent de cette progression [385 à 391]. L'étude des modèles d'affaires sur la base des rapports annuels des opérateurs de plateformes ou de télécommunications, ainsi que celle des contrats qui lient leurs services et sur des sources tierces permettent de dégager une variété de modèles d'affaires, lesquels ont des liens forts avec divers modes opératoires. Les modèles d'affaires sont étroitement liés aux motivations qui se trouvent dans la littérature et qui éclairent les motivations de certaines approches invasives en matière de GIDIM. Leur étude est couverte par un corpus académique dont le crépuscule se situe autour de 2010. L'ensemble des modes de gestion de l'identité, sur plateforme mobile ou non, vise la gestion de divers risques relatifs aux données. La littérature permet, par ailleurs, de recenser les

principales parties impliquées sur le sujet de la GIDIM, ainsi que les enjeux auxquelles elles sont associées.

Enfin, l'écart entre les principaux modes d'opération natifs des plateformes *iOS* et *Android* et les besoins et enjeux identifiés aux étapes précédentes commencent à être abordés par l'industrie, voire par l'Académie. À cet égard, les modèles Samsung Knox et (Google) *Take Out* sont bien documentés (et font également l'objet d'observation directe). Une brève étude élargie des avenues existantes complète le tout. À partir de ce stade, il faut synthétiser ce qui a été trouvé et l'exprimer en modèles de modes opératoires.

3.2 Élicitation des besoins et enjeux, élaboration et utilisation d'une grille d'analyse.

L'élicitation des besoins se fait à partir des enjeux trouvés dans la littérature. Ceux-ci sont organisés en une grille permettant d'analyser le positionnement des modes opératoires natifs des deux principales plateformes.

3.3 Sélection des principales plateformes et extensions

La sélection des principales plateformes s'est faite sur la base de la part de marché (*iOS* et *Android*) et les extensions retenues le sont également un peu sur cette base ainsi que sur celle de leur notoriété subjective. Bref, ces extensions représentent celles connues ou découvertes par l'auteur.

3.4 Observation des deux principales plateformes

Les activités d'observation des deux principales plateformes sont, somme toute, assez simples, elles visent à observer des appareils contenant la plus récente version stable du système d'exploitation de la plateforme. Attendu que ces observations ont été menées incrémentalement sur plus de dix (10) ans, il y a une riche collection de versions de ces observations, au fil du temps et des sorties des différentes versions des plateformes. Parfois,

des notes historiques pourront être présentées, lorsque pertinent. La présente version de ce mémoire ne fait cependant pas usage de la plupart de ces observations.

3.5 Élaboration des modes opératoires proposés

L'élaboration des modes opératoires proposés est un processus qui n'est pas formellement défini, mais qui consiste en une succession de cycles constituées des étapes suivantes : l'identification d'éléments d'observation des plateformes existantes, identification d'éléments d'insatisfaction provenant de la grille d'analyse basée sur les enjeux et besoins, proposition de changement, validation par rapport aux contraintes imposées par les modèles d'affaires. Il demeure inspiré du processus de Rzepka.

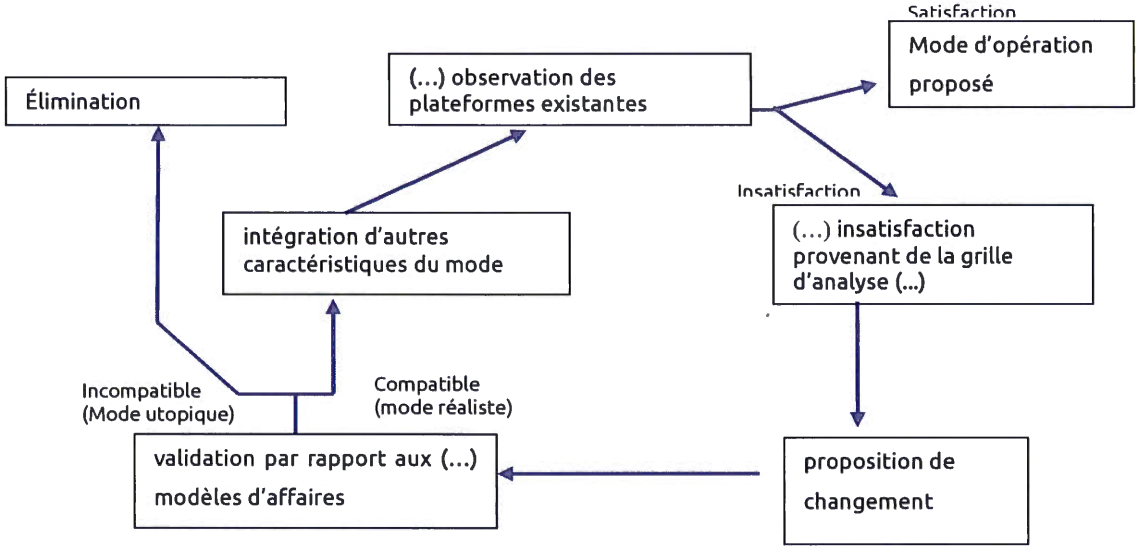


Figure 3.2 – Processus d'élaboration de modes d'opération

Dérivé de A REQUIREMENTS ENGINEERING TESTBED: CONCEPT AND STATUS, William E. Rzepka , 1989

3.6 Rattachement des modes opératoires

Le rattachement des modes d'opération à des modèles d'affaires ou à des rôles d'utilisation se fait comme conséquence du processus décrit en section [S: 3.5] ainsi que par exemplification. Il n'est pas requis que les données émanant du rattachement à des rôles soient ni exhaustives, ni exclusives, ce ne sont que des exemples. Dès qu'un exemple est trouvé, cela suffit.

3.7 Identification des extensions à élaborer

L'identification des extensions à élaborer se fait également par un processus similaire à celui documenté en section [S : 3.5], à l'exception qu'il est question de fonctionnalités et non de modes et qu'il n'est pas nécessaire de les confronter aux modèles d'affaires.

CHAPITRE IV

RÉSULTATS, LEUR ANALYSE ET LEUR DISCUSSION

4.1 Descriptif de la situation

4.1.1 Enjeux identifiés

Les trois sources pour les enjeux furent principalement les transcriptions de la Commission Chamberland, les débats sénatoriaux sur la confidentialité des sources journalistiques ainsi que le rapport *REISearch*.

Les principaux enjeux identifiés sont les suivants (sans ordre précis) :

01) la sécurité,
02) l'efficacité,
03) la souveraineté,
04) la temporalité,
05) la diversité,
06) l'ouverture et
07) l'importance.

La méthode ne permettant pas ni ne cherchant à obtenir de classement, les enjeux sont énoncés, mais sans qu'aucun ordre spécifique de leur soit dévolu. Notons que la sécurité revient souvent, mais celle-ci est souvent perçue différemment, voire aux opposés, par diverses parties. Ainsi, la capacité légale et technique d'intercepter les communications des cibles peut être vue par des membres de l'exécutif comme une fonction faisant partie de ses prérogatives relevant de la sécurité alors que pour ces mêmes cibles, c'est le composant « confidentialité » de la sécurité qui correspond davantage à leur idée du concept de la sécurité. D'autres notions ressortent telles la temporalité, laquelle dénote que la valeur des informations varie de manière importante au fil du temps. Ensuite, un autre enjeu qui semble important est celui, justement, de « l'importance ». Il semble y avoir une prise de conscience,

du côté de l'exécutif, à l'effet que de capturer des volumes trop grands d'information, même avec les meilleurs outils d'analyse disponibles ou à venir, peut être contreproductif du fait que la capacité cognitive des personnes en position décisionnelle est limitée et que les ressources d'application de la loi (« *enforcement* »), elles aussi, sont limitées.

4.1.2 Besoins identifiés et leurs métriques (non-ordinal)

De manière similaire, il a été possible, auprès des mêmes sources d'information auxquelles se sont rajoutées les éléments de la littérature références au cours de la revue de celle-ci, de dégager des besoins, ceux-ci sont plus précis que les enjeux, mais ne forment pas nécessairement un ensemble exploitable, cohérent et ordonné. Donc, encore une fois, c'est un ensemble sans ordonnancement qui est présenté. Voici donc les besoins recensés en matière de GIDI :

01) Assurer l'intégrité des processus et des résultats de GIDI contre les falsifications ou les erreurs.

02) Assurer la confidentialité des informations de GIDI contre les fuites (communications non- autorisées).

03) Assurer la confidentialité des données GIDI à la source, en ne permettant que leur prélèvement minimal nécessaire et en combattant le prélèvement abusif.

04) Assurer l'intégrité de l'information en rendant caduques les informations trop datées.

05) Assurer la confidentialité de l'information en favorisant le droit à l'oubli et en prévenant le caractère illimité de la permanence des données en ligne.

06) Assurer la disponibilité de l'information en imposant des obligations de conservation et des normes diverses et variées à ceux qui opèrent des activités de GIDI, afin de lutter contre l'indisponibilité de ce service jugé critique.

07) Assurer la disponibilité de l'information en ouvrant les normes, l'interopérabilité et l'accessibilité au statut d'acteur dans ce domaine aux petits joueurs, afin de contrer les risques d'oligopole.

08) Assurer la disponibilité de l'information en favorisant l'accès à la GIDI dans les régions éloignées, afin de combattre le risque d'exclusion sociale de larges portions de la population.

09) Assurer la souveraineté numérique de la nation.

10) Assurer l'auto-détermination numérique individuelle.

Au Canada, ce sont principalement les points 1, 2, 3,6, 7 et 8 qui semblent encouragées par l'État. Au niveau provincial (Québec), ce sont les points 1, 2, 3 et 6 qui semblent visés.

Encore une fois, il semble y avoir une bonne concordance entre les besoins exprimés et la situation actuelle. Il n'a pas été mis en hypothèse que l'inadéquation était totale ou dominante. Il est uniquement question d'apporter des améliorations afin de permettre d'exprimer, dans la conception et l'exploitation des appareils mobiles, les besoins des UFs en matière de GIDIM.

Chaque partie reconnaît la pertinence des points de vue des autres, notamment du fait que l'exécutif est investi d'autorité par le législatif, lequel a aussi voté des lois pour protéger les droits des individus. Similairement, ceux-ci sont conscients de l'utilité de l'efficacité de l'exécutif. Il est donc question de négociation des limites des prérogatives. C'est un travail d'ajustement important, mais loin d'être acrimonieux. Peut-être la composition et le caractère la société québécoise peuvent expliquer le caractère paisible de ces échanges.

Pour qu'un tel échange rationnel et productif ait lieu, il faut des indicateurs de succès. À la base, ceux-ci ont besoin de métriques et d'unités de mesures. Pour chacun de ces besoins, il peut y avoir des métriques dérivées permettant de mesurer le niveau auquel ces besoins sont comblés. Ceux-ci ne sont pas nécessairement en corrélation 1-à-1 avec es besoins, ils peut y avoir des partages et des chevauchements.

Métriques relatives aux besoins :

01) Ratios d'efficacité (faux positifs, faux négatifs, etc.)
02) [Voir 01]
03) Volumétrie (bits) des captures d'infos de GIDIM
04) Le bit x seconde (produits de la quantité d'information par sa durée de rétention)
05) Taux de réussite des normes; coefficient de difficulté/échec des exigences
06) [Voir 05]
07) Variance et distances totales dans les coordonnées représentant les acteurs
08) Coefficient de couverture en fonction des coordonnées géographiques
09) Variance et distances totales dans les coordonnées représentant les acteurs dans un espace adapté aux considérations politiques.
10) Taux de satisfaction relativement à cette question.

4.1.3 État de la sphère judiciaire

Le dernier résultat qu'il est à propos de présenter pour témoigner de la situation actuelle, dans le but de comprendre les résultats suivants découlant de la phase d'analyse et de synthèse, concerne l'état de la sphère judiciaire. Le processus anticipatif débute avec toutes les considérations à savoir si le bras armé de l'État (son exécutif), le plus souvent au travers de l'un ou l'autre des services de police de son territoire, peut intervenir dans les appareils mobiles des citoyens. À l'autre bout du processus judiciaire, il y a les considérations relatives à la possibilité que ces données ainsi recueillies soient utilisées et admises devant une instance judiciaire pour déterminer la culpabilité relativement à un fait reproché ou pour fixer une peine. Également, attendu que c'est aussi le judiciaire qui, dès le début du processus garantit le respect des droits constitutionnels (systémiques) des citoyens, il est également intéressant à ce chapitre de connaître l'état de la situation sur le sujet.

Tableau 4.1 – Fréquence des occurrences des termes sur le portail CanLii en 2016

Expression	Nombre d'occurrences
iPhone	194
iOS	20
Android	49
Facebook	2 028
Twitter*	88
LinkedIn	63
Firefox	2
Outlook	240
Password	99
"Mot de passe"	798
EXIF	0
Tinder	1
"Ashley Madison"	0
"Réseau Contact"	26

Les résultats présentés au tableau [S : 4.1] illustrent le fait que les tribunaux agissent de plus en plus dans la sphère numérique. Notamment, ils y puisent nombre d'éléments de preuve. Cela ne se limite pas au cadre pénal, mais aussi au civil. Par exemple, les publications *Facebook* publiques sont admissibles en preuve et nourrissent de plus en plus la capacité probante, à charge ou à décharge. Par exemple, un « *check-in* » (enregistrement géographique) peut faire pencher la balance, sur la base de la prépondérance de la preuve, en faveur d'utilisateur dont l'employeur remet en question la présence au travail. À l'inverse, un assureur peut voir dans les photos de voyage, publiées, une preuve de l'inadmissibilité d'un autre justiciable qui se prétend inapte au travail.

Toutes ces observations convergent pour mettre de l'avant le caractère souvent indélébile des traces que les individus laissent sur Internet, de là l'importance que ceux-ci aient un certain contrôle sur ces données et que des outils existent et soient mis en œuvre au bon niveau afin de leur permettre de prendre les bonnes décisions.

Tableau 4.2 – Résultats des demandes de mandats judiciaires d'accès aux données (2009-2013)

Condition ou refus	Nombre de demandes				
	2009	**2010**	**2011**	**2012**	**2013**
Sous conditions	140	114	135	108	120
Sans conditions	1	1	2	4	3
Refus	0	0	0	0	0

Les résultats de ce deuxième tableau sont les plus troublants ou du moins étonnants. Ils concernent les statistiques obtenues du Rapport annuel sur la surveillance électronique – 2013 [416]. Elles apportent l'éclairage à l'effet qu'absolument aucune demande n'a été refusée pendant la période couverte. Des préoccupations similaires sur la facilité d'obtention d'une autorisation judiciaire d'écoute ont également été exprimées lors des audiences de la Commission Chamberland ainsi qu'en matière de coopération entre les états membres de l'UE dans les groupes de discussion de *REISearch*. Ces données peuvent contraster avec une présomption que certains utilisateurs ont peut-être à l'effet que l'obtention d'un mandat est un filtre sévère et éliminatoire serré.

4.2 Grilles d'analyse des plateformes

Les quelques prochaines pages présenteront des grilles permettant d'exprimer les résultats des activités de synthèse en comparant les principales plateformes, *Android* et *iOS*. Le tableau présentant les grilles [S: 4.2.1] et [S: 4.2.2] expriment les résultats des observations menées par des analyses d'informatique judiciaires menées avec les logiciels *Sekomon*, *Encase* (Mobile) et FTK ainsi qu'avec les utilitaires Linux ordinaires *dd*, *cat* et *xxd*. Elles expriment la synthèse des principales catégories de données recensées dans la littérature référenciée et pour chaque élément, des observations ont été menées afin de voir si ces données sont trouvées (même sous une forme transformée) et si elles sont interceptées en communication (au travers l'outil *Sekomon* et *Apache* utilisé en tant que Proxy judiciaire afin de permettre la substitution de certificats et de permettre ainsi la lecture de certaines données communiquées). Pour iOS, les plateformes étudiées ont été celles du *iPhone* et du *iPod Touch* roulant sous iOS 5, 6, 7, 8 et 9. Pour Android, l'étude a été menée sur le *Samsung Galaxy S3*

(modèele GT-i9100 xxxx distribution canadienne) pour les versions d'*Android* allant de 4.1 à 5.0, puis sur le *Samsung Galaxy S4* (GT-i9505 xxxx, distribution canadienne) pour les versions d'A*ndroid* 5.0 et 6.0. Une observation positive (« Oui ») est recensée dès que l'élément apparaît ou est documenté dans l'une ou l'autre des versions analysées.

Ensuite, vient une série d'intégrations d'éléments qui permettent d'illustrer la couverture ainsi que les déficits observés, par rapport aux besoins identifiés, sur les diverses déclinaisons des plateformes existantes ainsi que par les dérivées de la plateforme *Android*, puis des autres extensions.

Le but de ces grilles d'analyse est de permettre au lecteur de constater qu'il y a eu des évolutions importantes depuis l'introduction de la plateforme Knox, mais qu'il subsistes des manques.

Tableau 4.3 – Données identifiées (4.2.1) et leur communication (4.2.2)

	Trouvé sur			
Type de données	***iOS***		***Android***	
Les données imputées	Résid.	Comm.	Résid.	Comm.
Nom d'usager (« *username* »)	Oui	Oui	Oui	Oui
Identifiant unique d'utilisateur	Oui	Oui	Oui	Oui
Identifiant de session	Oui	Oui	Oui	Oui
Identifiant de point de contact	Oui	Oui	Oui	Oui
Nom légal	Oui	Oui	Oui	Non
Âge légal ou date de naissance	Oui	Oui	Oui	Oui
Le mot de passe ou un dérivé	Oui	Oui	Oui	Oui
Le genre/sexe légal ou un dérivé	Oui	Non	Oui	Non
Les questions de sécurité				
Les informations sociales adjacentes	Oui	Oui	Non	Non
Les applications installées	Oui	Oui	Oui	Oui
Les informations système (versions)	Oui	Oui	Oui	Oui
Le contenu créé (et non-capturé) par l'utilisateur				
Les notes	Oui	Oui	Oui	Oui
L'emploi du temps	Oui	Oui	Oui	Oui
Les recherches	Oui	Oui	Oui	Oui
Les données relatives aux communications				
Le contrôle de la carte SIM et de l'IMEI	Oui	Oui	Oui	Oui
Les appels	Oui	Oui	Oui	Oui
Les textos	Oui	Oui	Oui	Oui
Les courriels	Oui	Oui	Oui	Oui
La navigation web	Oui	Oui	Oui	Oui
Les télécommunications (leur topologie)	Oui	Oui	Oui	Oui

Tableau 4.3 – Données identifiées (4.2.1) et leur communication (4.2.2) – suite et fin

	Trouvé sur			
Type de données	***iOS***		***Android***	
Les données (...) communications (suite et fin)	Résid.	Comm.	Résid.	Comm.
Les réseaux WiFi	Oui	Oui	Oui	Oui
Les réseaux Bluetooth	Oui	Oui	Oui	Oui
Les points NFC et RFID (le cas échéant)	Oui	Non	Oui	Non
Les réseaux cellulaires	Oui	Oui	Oui	Oui
Les données relatives à la position				
Distance d'un émetteur GPS	S/O	S/O	S/O	S/O
Distance d'un réseau (constellation) d'émetteurs GPS permettant de trianguler le signal	Oui	Oui	Oui	Oui
Les données des capteurs				
Les données sur la luminosité	Oui	Oui	Oui	Non
Les données sur la proximité	Oui	Non	Oui	Non
Les données capturées par le microphone (son.)	Oui	Oui	Oui	Oui
Les données capturées par la (les) caméra(s)	Oui	Oui	Oui	Oui
Certaines données d'instrumentation				
L'utilisation de l'appareil	Oui	Oui	Oui	Oui
L'accélération de l'appareil	Non	Oui	Non	Non
Les données relatives au branchement électrique	Oui	Oui	Oui	Oui*
Les données relatives à l'affichage	Oui	Oui	Oui	Oui*
Autres capteurs				
Les empreintes digitales	Non	Non	Non	Non
Humidité et température	Non	Non	Non	Non
Les diverses pressions (atmosphérique, écran, etc.)	Non	Non	Non	Non
Le pouls de l'UF (*Apple Watch*, *FitBit*, etc.)	Oui	Oui	Non	Non
Autres données				
Données externes	S/O	S/O	S/O	S/O
Données de tiers	Oui	Oui	Oui	Oui
Données tertiaires (composées)	Oui	Oui	Oui	Oui

4.2.3 Clientèles

Les principales (* : voir note 1, en page [P : 125]) clientèles suivantes ont été identifiées, elles ne représentent cependant pas une partition ni exclusive, ni exhaustive de la population :

1) Les utilisateurs personnels

Les utilisateurs ordinaires qui utilisent les appareils mobiles à des fins ludiques et personnelles, ce qui peut notamment inclure la supervision parentale exercée sur autrui. Il n'y a pas de hiérarchie entre les utilisateurs, mais il peut y avoir des rapports de confiance.

2) Les utilisateurs professionnels « légitimes »

Il s'agit d'une clientèle qui utilise les appareils mobiles comme outil d'un travail ordinaire qui ne soit pas versé dans l'informatique (mobile en particulier) et où il y a une notion de responsabilité professionnelle face à l'information (ex : dossier médicaux pour un médecin, stratégies judiciaires pour un avocat, etc.). Il pourrait y avoir des distinctions faites entre les employés (qui n'ont pas de contrôle) et les travailleurs autonomes (qui, dans une certaine mesure, peuvent l'avoir).

3) Les individus vulnérables et sous assistance (enfants, aînés, personnes sous tutelle ou curatelle)

Il s'agit d'individus vulnérables dont l'utilisation des plateformes mobiles est sujette au contrôle d'autrui et où les droits individuels sont également attribués à ce tiers présumé de confiance.

4) Les représentants politiques

Il s'agit d'une catégorie d'utilisateurs assez similaire à celle des utilisateurs professionnels, mais qui encourt un profil de risque particulier du fait qu'il se trouve exposé davantage à des risques d'intrusion d'État (de la part de factions concurrentes ou d'États concurrents) ou privée, essentiellement due à une possible influence politique étant recherchée par de telles intrusions.

5) Les utilisateurs techniques de service (développeurs, testeurs, etc.)

Il s'agit d'une autre clientèle assez proche de la clientèle professionnelle, mais qui a comme particularité d'être à la base des activités de développement sur plateformes mobiles. Il y a donc une utilisation souvent dépourvue de contexte personnel. Par exemple, si ces utilisateurs créent un compte dont le prénom est « Test », il n'y a généralement pas de volonté de fournir des renseignements erronés ou frauduleux, mais simplement de pouvoir mener des tests sur la plateforme. Notons que cette clientèle est techniquement apte à modifier la plateforme elle-même.

6) Les utilisateurs professionnels ou engagés, interlopes

Voilà une catégorie redoutée et pourchassée par l'État. Il s'agit d'utilisateurs dont l'utilisation des technologies mobiles vise des buts contraires aux normes sociales communément établies. Ce segment de clientèle regroupe tant les consommateurs que les fournisseurs de ce milieu, qu'il s'agisse de commerce de stupéfiants, de marchandisation du sexe ou bien de diffusion de contenu haineux ou faisant l'apologie du terrorisme.

7) Les utilisateurs académiques

Cette catégorie regroupe petits et grands, tant que leur utilisation est centrée autour des activités d'apprentissage orchestrées et encadrées par une institution dûment reconnue d'apprentissage auprès de laquelle ils sont membres. Leur utilisation est au carrefour entre une fonction de grande utilité sociale, l'exercice du droit à l'éducation et l'utilisation de

technologies privées sous le contrôle de l'institution. Les parties prenantes sont alors multiples et les besoins complexes.

8) Les utilisateurs de surveillance et d'audit

Il s'agit d'une type d'utilisateur qui exerce de l'autorité sur d'autres utilisateurs, le plus souvent pour le compte d'un tiers constitué (ex : employeur). L'utilisation par cette clientèle a deux caractéristiques : elle devrait être tenue à des normes éthiques dans l'exercice de ses fonctions d'autorité et elle présente un potentiel de risque plus élevé parce qu'il s'agit d'une cible de choix pour des pirates.

9) Les utilisateurs atypiques (partages de compte, comptes d'essai, etc.)

Il s'agit ici de la clientèle dont l'utilisation est atypique et souvent non-conforme aux politiques d'utilisation. Cela inclut notamment les systèmes automatisés pour lesquels un compte a été créé, les automates, les associations ainsi que les utilisations partagées, telles celles par un couple, une famille ou un individu agissant au nom d'un tiers (ex : compte opéré par le petit-fils pour la grand-mère, sans mandat d'inaptitude formel). Cette clientèle inclut aussi toute clientèle résiduelle ne pouvant mieux se classer ailleurs ou autrement du fait de son caractère atypique.

10) Les migrants

Il s'agit d'une clientèle vulnérable et qui, depuis la crise humanitaire syrienne présente une particularité intéressante dans le contexte de la GIDIM : ils présentent une scolarisation supérieure et une utilisation des TIC (et des TIC mobiles en particulier), assez soutenue. C'est une clientèle qui s'engage parfois dans des activités illégales (en matière d'immigration) ainsi que dans des interactions avec des professionnels du monde interlope (ex : les passeurs) et dont l'utilisation des technologies mobiles constitue un aspect important de leur expérience de migrant. Bref, ils correspondent au terme « réfugié branché » (« *digital refugee* ») tels que proposé dans un article soumis à la *Harvard Business Scool* [392] et au *Pew Research Center* (2017) [393].

* Note 1 : La clientèle des réfugiés ne présente pas, dans l'absolu, et en particulier au Québec, un segment statistiquement significatif de la population. Or, il est retenu comme une « clientèle » du fait qu'il existe des développements particulièrement intéressants (système biométrique du Commissariat des Nations Unies aux Réfugiés, « *UNHCR BIMS* ») relatifs à la GIDI(M) de ce segment de la population et qu'il s'agit d'une clientèle particulièrement connectée et vulnérable à certains risques identifiés comme émanant du contrôle de l'État.

4.2.4 Évaluation de la satisfaction des besoins recensés par les modes d'opération disponibles

Une fois les clientèles connues et leurs besoins recensés collectivement, il est possible de s'adonner à la tâche d'évaluer les modes d'opération par défaut des différentes plateformes afin de voir s'ils y sont intégrés, soit dans la littérature, soit dans le fonctionnement observé. Les résultats se trouvent ci-bas, le succès étant accordé lorsque ce besoin est spécifiquement satisfait dans la version de base de la plateforme sans aide de quelque application ou configuration que ce soit.

Tableau 4.4 – Visualisation comparative entre les modèles des besoins et les modèles de modes d'opération

Besoin #	*iOS*			*Android*		
	Ordinaire	Sans ID	*jailbreak*	Ordinaire	Sans ID	*rooted*
1	**Succès**	SO	**Échec**	**Succès**	SO	**Succès**
2	**Succès**	**Échec**	**Échec**	**Succès**	**Échec**	**Échec**
3	**Échec**	**Échec**	**Échec**	**Échec**	**Échec**	**Échec**
4	Mitigé	**Échec**	**Échec**	Mitigé	**Échec**	**Échec**
5	**Échec**	**Échec**	**Échec**	**Échec**	**Échec**	**Échec**
6	**Échec**	SO	**Échec**	**Échec**	**Échec**	**Échec**
7	**Échec**	SO	**Échec**	**Succès**	SO	**Succès**
8	SO	SO	SO	SO	SO	SO
9	**Échec**	**Échec**	**Échec**	**Échec**	SO	**Échec**
10	**Échec**	**Échec**	**Échec**	**Échec**	**Échec**	**Échec**

Légende : Succès : répond spécifiquement à ce besoin ;
Échec : ne répond pas spécifiquement à ce besoin
Mitigé : répond avec un succès mitigé à ce besoin selon les (sous) versions
SO : Sans objet; ce besoin n'est pas applicable en l'espèce.
Note : Le point #9 est évalué d'une perspective canadienne.

4.2.5 Principales couvertures

La situation actuelle démontre que les mécanismes de GIDIM déployés sur les principales déclinaisons des principales plateformes sont, somme toute, assez sommaires. Ils permettent de s'acquitter de la principale fonction de GIDIM, essentiellement l'authentification et un certain contrôle des accès (facilement compromissible si on n'utilise pas d'encryption). Google offre, de par sa compatibilité avec *OAuth*, une meilleure posture théorique face aux risques liés aux oligopoles, mais dans les faits, la situation est similaire à celle d'*Apple*.

4.2.6 Principales déficiences

Il y a de nombreux échecs, en utilisant cette grille d'évaluation. Cela semble contredire le niveau de satisfaction générale assez élevée des utilisateurs, du moins des utilisateurs québécois, ce qui risque de soulever la question de la pertinence de la grille d'analyse. Cela est vrai, mais pour apprécier la validité de la chose, il faut prendre une certaine distance et suivre ce qui se fait comme développement dans d'autres pays, notamment en Chine ou dans certains pays d'Europe, où on se méfie davantage du manque de diversité des fournisseurs et de leur concentration d'intérêts politiques en Amérique du Nord. Ensuite, il faut garder à l'esprit que l'adoption, voire la satisfaction générale à l'égard d'un produit n'équivaut pas à l'absence d'insatisfactions particulières à son égard, surtout lorsque les choix sont restreints.

Bref, ce n'est que lorsqu'ils sont sondés spécifiquement sur la problématique que les UFs expriment des insatisfactions, malgré un usage généralement satisfaisant. Aussi, ce qui permet de se rassurer par rapport à un éventuel biais introduit par la question, c'est le caractère articulé et diversifié des réponses obtenues. Il demeure cependant pertinent d'approfondir la validation de cette partie des résultats.

4.2.7 Principales évolutions

Il est à anticiper que la lecture proposée de la situation soit partagée par d'autres acteurs sur la scène du développement mobile et que, en conséquence, ces développeurs aient entrepris divers efforts visant à améliorer cette situation. Que tel soit le cas où que les motivations soient toutes autres, la présente section présente les principales extensions, évolutions et adaptations qui divergent de réalité initiale de la plateforme *Android*. Notons que cette attention particulière et asymétrique par rapport à *iOS* est simplement due au fait que, *iOS* étant propriétaire, il n'y a pas de version dérivée légitime, ni même présentant une adoption significative.

Une fois ces antécédents étayés, voici donc les principales extensions dérivées de la plateforme *Android* et rencontrées dans la littérature :

Les Mods

Lineage(OS) : *Lineage* est une version émanant de CyanogenMod suite à la fin de cette dernière.

Cyanogen : *CyanogenMod* est une version dérivée du matriciel (« *firmware* ») *Android* de base permettant d'évacuer l'omniprésence des services Google et offrant des utilités telles le « *rooting* », mais aussi sauvegarde intégrale, etc. Le développement de cette mod est présentement abandonné au profit d'une version qui en est le successeur (« *LineageOS* »).

Oxygen / Hydrogen : *Oxygen* et *Hydrogen* sont également des versions dérivées ou inspirées de CyanogenMod et qui ont été principalement développées, promues et déployées par OnePlus, un fabriquant d'appareils mobiles soucieux des considérations de performance, de protection de la vie privée et de la souveraineté nationale des utilisateurs, dont un nombre important sont Chinois ou issus de pays autres que les États-Unis d'Amérique. Notons que ces deux versions supportent les modes d'opérations basés sur *Android* SE proposés par Smalley.

Replicant : Il s'agit d'une version alternative qui remplace tout le contenu propriétaire d'*Android* par des substituts totalement libres de droits et de code source ouvert.

Smartizan : Cette version est une version alternative dont le développement a fait suite à celui d'Oxygen, lequel a induit une vague importante d'efforts de développement de versions alternatives sinophiles, orientées autour des besoins des utilisateurs chinois. On trouve dans cette vague également MIUI ainsi que FlyMe (par Meizu), ce dernier couvrant une part de marché, somme toute, assez restreinte.

MIUI :Il s'agit de la version alternative la plus développée parmi celles ayant émergé de l'envol sinophile/sinisant. Notons que l'importance de cette version est fortement associée au segment du marché occupé par les petits fabricants de matériel qui n'ont pas grande voix au chapitre de la *Open Handheld Alliance*, et possiblement en réaction à la mainmise de Google sur cette association qui se devait d'être libre.

Copperhead : Il s'agit d'une version qui est conçue avec la protection des renseignements personnels et la sécurité comme principales préoccupations. Elle offre notamment les modes basés sur *Android* SE proposés par Smalley.

Autres extensions

F-Droid : Il s'agit d'un pendant structuré et organisé visant à concurrencer *Google Play (Store)* comme source d'applications, le tout sous des contraintes à l'effet que les applications distribuées soient exclusivement en code source ouvert et libres de droits.

Orbot : Il s'agit d'une version pour *Android* du logiciel Tor, incluant bien entendu le navigateur anonyme *Tor Browser*, mais capturant l'ensemble du trafic réseau de l'appareil pour l'obfusquer et offrant aussi des fonctionnalités de messagerie et de communication VoIP. Notons que des applications similaires existent sous *iOS*, mais de par la conception du modèle de sécurité d'*iOS*, celles-ci ne permettent pas une capture de l'ensemble du trafic.

Apps de migration de données : Le modèle de sécurité d'*iOS* ne le permettant pas, seulement sur *Android* sont disponibles des applications permettant l'extraction et la sauvegarde de données telles le registre des appels, la base de données des contacts et des SMS/MMS+, etc.

Autres évolutions

À part les extensions formelles et structurées mentionnés plus haut, il existe de timides évolutions ici et là qui sont dignes d'être mentionnés et intégrées aux extensions proposées. Celles retenues ont essentiellement des évolutions physiques visant à répondre à des besoins spécifiques. Par exemple, l'addition d'un témoin lumineux (LED) permettant de savoir quand la caméra ou le Wifi sont en fonction présentent d'intéressantes évolutions. De la même manière, l'introduction d'un interrupteur physique permettant de s'assurer que l'appareil est vraiment électriquement éteint vont dans le même sens. Enfin, l'utilisation de pellicule-discrétion (« *privacy film* ») sur l'écran des appareils mobiles afin de protéger contre les yeux indiscrets présentent une dernière évolution digne de mention.

Tableau 4.5 – Grille d'analyse enrichie des extensions dérivées et spécialisées telles qu'observées (4.2.8)

Besoin #	*Android*					
	Lineage/ Cyanogen	Hydrogen/ Oxygen	Replicant	Knox	Smartizan & MIUI	Copperhead
1	-	=	-	+	=	+
2	+	+	=	+	+	+
3	+	+	SO	+	SO	+
4	SO	SO	SO	SO	SO	SO
5	SO	SO	SO	SO	SO	SO
6	SO	SO	SO	SO	SO	SO
7	+	+	+	+	+	SO
8	SO	SO	SO	SO	SO	SO
9	+	+	=	=	+	SO
10	+	+	+	=	-	+

Légende :
+ : correspond a une couverture améliorée par rapport au mode natif de la plateforme *Android*
- :correspond a une couverture détériorée par rapport au mode natif de la plateforme *Android*
= : correspond a une couverture inchangée par rapport au mode natif de la plateforme *Android*
SO : Sans objet; ce besoin n'est pas applicable en l'espèce.
Vert correspond à une situation de succès
Ambre correspond à une situation mitigée
Rouge correspond à une situation d'échec
Note : Le point #9 est évalué d'une perspective canadienne.

4.3 Présentation des nouveaux concepts nécessaires à l'extension des plateformes et spécifiques à la GIDIM

Les concepts suivants ne se trouvent pas toujours explicitement identifiés, définis et étudiés formellement dans la littérature, mais leurs éléments s'y trouvent et il ne manque parfois que leur assemblage afin de débuter leur étude. Tout comme les concepts nécessaires à la revue de la littérature ont permis de connaître la situation actuelle, les concepts présentés dans cette section permettent, à ce stade, de l'étendre.

4.3.1 Point de contact neutre [394 et 395]

Le concept derrière le point de contact neutre est simple : il s'agit d'un dispositif doué d'une interface personne-machine qui soit dépourvu de tout logiciel visant à mettre en place des politiques unilatérales d'une partie (incluant son fabriquant et son opérateur de plateforme) et dont la conformité à une norme ne serve qu'à assurer un déploiement conforme de l'identité ou des identités dûment autorisés sur celui-ci, exclusivement pour la durée de la session. Cet appareil est comme un lecteur de CDs qui se contente de lire l'identité qui est téléchargée d'un serveur après authentification ou fournie avec les certificats appropriés. Ainsi, ce dispositif ne doit pas avoir de propension programmée de manière à avantager qui que ce soit, il doit être neutre. Il doit aussi être amnésique, dans la mesure où, une fois l'identité ayant terminé la session, il ne doit rester aucune trace de l'expérience qui vient de se dérouler sur ce dispositif. Tout au plus, il doit offrir des garanties contre la subversion d'appareil (« *device tampering* »).

4.3.2 Identité portable [396]

Une identité portable en est une qui soit indépendante de la mise en œuvre matérielle ou logicielle et qui puisse être portée d'une plateforme à une autre. Le principal problème lié à l'expansion de l'adoption de ce concept est que le nombre d'utilisateurs est un marqueur de

pouvoir et de valeur pour les entreprises [397 et 398], ainsi qu'un facteur de rétention de la clientèle et des revenus qui l'accompagnent.

4.3.3 Témoin matériel direct

Il s'agit d'un indicateur matériel qui ne soit pas programmable, mais qui permette plutôt d'afficher, directement, l'utilisation d'une ressource. Par exemple, lorsque l'on active une webcam [399 et 400], il peut y avoir un témoin insuppressible, par exemple sous la forme d'une lumière rouge qui clignote, qui avertit l'utilisateur que la caméra web fonctionne. Similairement, on peut avoir des témoins qui attestent de l'état électriquement éteint de l'appareil, de la capture du microphone, de l'activité du capteur GPS, de l'état « mode avion » ou « mode Faraday », ou de réalités plus complexes comme l'utilisation d'un proxy sécurisé ou la compromission possible d'un appareil ou d'un service, dans lequel cas, ces témoins matériels ne seraient pas toujours directs, ou seraient directs, mais en lien avec des composants spécialisés, tels un module d'informatique de confiance (« *trusted computing* »). Il est à noter que la principale qualité de ces témoins est leur inconditionnalité, qu'ils ne puissent pas afficher un état qui ne corresponde pas à la réalité.

4.3.4 Stratégies de segmentation anti-collusion

Les stratégies anti-collusions sont des stratégies de segmentation de l'information ou du traitement qui permettent de mitiger une situation d'absence de confiance (« *zero trust* »), par exemple, lorsque l'on fait utilisation de services d'infonuagie de la part de fournisseurs pouvant être hostiles ou compromis. Il est à noter que ce ne sont pas toutes les fonctions de traitement qui peuvent être assujetties à ces stratégies. Les plus récents travaux cités à quelques reprises dans ce domaine sont ceux de Z. Zhu, de Z Cao [401] et de Ramesh Kumar [402].

4.3.5 Service d'assistant automatisé virtuel

Ce concept a été introduit dès le début du présent mémoire et vise un ensemble de logiciels organisés en service de manière à offrir à un utilisateur individuel, ou à un ensemble d'utilisateurs dans le cas d'utilisation groupée, des services de traitement centrés sur l'interaction avec d'autres plateformes électroniques afin d'optimiser l'avantage dudit utilisateur et de défendre ses intérêts et avantages.

Par exemple, lors d'une enchère, un assistant automatisé virtuel peut émettre des offres successives jusqu'à concurrence de la limite fixée par l'utilisateur. Dans une autre instance, il pourrait chercher des stationnements pendant que l'utilisateur arrive à son restaurant préféré. Similairement, il pourrait lire les complexes conditions d'utilisation et recommander l'installation d'une application ou non, ou bien procéder à l'installation et s'assurer que certains senseurs ne capturent ni communiquent certaines données. Il pourrait même répondre des mondanités à certains contacts dudit utilisateur. Pour ce faire, cet assistant devrait vraisemblablement disposer de trois choses : des mécanismes d'intelligence artificielle, des données très détaillées sur l'utilisateur et des données externes très fournies : cartographie, prix et cotes, actualités, accès à des répositoires de nouveaux apprentissages, données de mise à jour, etc. L'intime connaissance des utilisateurs en fait une cible de choix pour les compromissions. Or, ce risque présente un avantage par rapport à la certitude actuelle à l'effet que le même rôle soit joué par des corporations à but lucratif qui ne visent pas à défendre d'abord les intérêts des utilisateurs. À ce chapitre, ce genre d'appareil ou de service ne devrait pas être fourni gratuitement, même et surtout par l'État, et devrait avoir comme seule allégeance celle envers l'utilisateur qu'il sert et « défend ». Cela rend une telle offre difficile à commercialiser avec les modèles d'affaires actuels et, puisque vraisemblablement, cela se base sur l'utilisateur-payeur, il serait à craindre que les inégalités de moyens puissent un jour aboutir en des inégalités en droit, certains pouvant se permettre de meilleurs assistants que d'autres.

4.3.6 Monétiseur des opérations

Il s'agit d'un dispositif logiciel qui permette d'accorder une valeur monétaire aux diverses opérations, dont à celles de GIDIM., Dans un contexte d'infonuagie, d'Internet des Objets ou de contrats intelligents, un tel dispositif joue deux rôles : il étend le concept d'entente de niveau de service (« SLA », « *service level agreement* ») pour les ressources que l'utilisateur consomme, mais il s'assure aussi d'obtenir quelque chose en échange des données dévoilées et de l'utilisation ou de l'inféodation à divers services auprès des divers opérateurs de plateforme, notamment les services de GIDIM. Bref, ce dispositif est la forme la plus élémentaire et commerciale d'assistant automatisé virtuel.

4.3.7 Mode d'opération

Un mode d'opération est un ensemble de paramètres qui permettent, dans un contexte, d'assurer une exploitation conforme d'un appareil aux attentes circonstancielles de l'utilisateur. Par exemple, lorsqu'un utilisateur est en mode « familial », ce ne sont que son contenu, ses paramètres et ses communications familiales qui sont disponibles et visibles. Si l'utilisateur est en mode « travail », ce sont les paramètres liés au travail qui sont mis de l'avant. Aussi, si l'utilisateur est en mode « sécurisé », il n'aura peut-être pas accès à ses copies pirates de films, mais il sait qu'il peut autoriser en toute confiance les transactions effectuées avec sa banque. Enfin, il peut aussi être dans un mode d'opération « individuel » ou « secret ». Un mode d'utilisation peut être lié à un témoin matériel (ex : lumineux), de manière à assurer l'UF qu'il est bien dans le mode qu'il croit être.

4.4 Approche par modes d'opération

L'aboutissement de la présente étude vise à apporter des améliorations afin de permettre de combler les écarts entre la situation actuelle en matière de GIDIM et les besoins tels qu'exprimés, notamment dans la littérature, mais également auprès des autres sources dont il a été abondamment question dès le début du présent mémoire. La nature de ces besoins

est trop diverse pour être contenue dans un faisceau cohérent de requis, le requis qui en émane donc est de permettre une conformité à une diversité de modes d'opération, également appelés des modes opératoires, qui correspondent à des profils non-exclusifs, voire transitaires, que les utilisateurs peuvent adopter.

Par analogie, c'est comme si, pour un appareil photo, on avait identifié des modes de prise de vue correspondant aux principales utilisations qui sont faites par les utilisateurs de l'appareil. Bien entendu, il serait encore plus adéquat de permettre un mode « manuel », permettant à l'utilisateur de contrôler lui-même exclusivement, en seul maître à bord, l'ensemble des activités de GIDIM et de collecte de données. Or, bien que diverses options et moutures d'offres de service semblent s'en rapprocher, cette option est fondamentalement indisponible puisque l'identité étant un concept relatif, la GIDIM est une activité qui se joue à plus d'un et, dans la situation actuelle, les OPs sont inflexibles à plusieurs égards en matière de GIDIM, principalement pour des motifs de sécurité et de responsabilité Par exemple, il n'y a pas un processus formel permettant de choisir un tiers de confiance afin de permettre, en cas de compromission du compte, de départager l'authentique de l'intrus. Par ailleurs, l'adoption touts azimuts d'un tel mode d'opération manuel pourrait compromettre la viabilité de plusieurs modèles d'affaires, ce qui semble être le motif officieux derrière cette inflexibilité que la limitation technologique ne justifie aucunement. Enfin, un mode manuel ou trop privé pourrait compromettre la capacité de l'État de jouer son rôle régalien, notamment en matière de protection.

La présente sous-section propose donc une liste de modes opératoires qui constituent des compromis viables eu égard les modèles d'affaires auxquels ils sont rattachés, et qui pourraient correspondre également à des clientèles particulières. Ces modes ne constituent pas une palette exhaustive, ni une partition exclusive, ils ne font que cadrer les principaux types d'utilisation d'une manière viable à l'égard des considérations discutés plus haut. Certains modes peuvent se chevaucher. Suivant la liste de ces modes, il y aura une analyse concernant les transitions entre ces modes, puis une brève réflexion sur la gestion de ces modes et rôles. L'exhaustivité serait, dans l'absolu, visée, sans être atteinte. Le but est d'avoir une couverture significative des types d'utilisations, principalement afin d'éviter des faiblesses. De nos jours, tant les leaders du monde libre que les milliardaires partagent, en

matière de GIDIM, les mêmes options restreintes que de simples adolescents et cela résulte dans une conformation de la réalité d'affaires aux options techniques disponibles, laissant de nombreux écarts. La formulation de ces modes est descriptive, elle décrit la nature du rôle, mais aussi normative, c'est-à-dire qu'elle doit énoncer les caractéristiques exigées de ce rôle.

Par la suite, il faudra établir un cadre robuste de gestion et de transition entre ces modes puisque certains sont inconciliables entre eux. Au départ, il y avait des besoins inconciliables qui ne présentaient pas un tout cohérent. À ce stade, on a des modes, parfois contradictoires si pris par paires, mais conciliables si pris dans leur ensemble. C'est à ce moment que le génie logiciel cède la place à l'informatique de gestion et que ce sont les processus de cette discipline qui permettent d'encadrer ces considérations relevant davantage du « quoi ? » (réalité d'affaires) que du « comment ? » (mise en œuvre selon les préceptes et les rigueurs du GL).

Modes d'opération proposés

4.4.1 Mode ordinaire (par défaut)

Il s'agit du mode actuel, lequel semble convenir à nombre d'utilisateurs et qui laisse une grande part de contrôle et de discrétion à l'OP. Rien ne justifie de voir disparaître ce mode et il constitue le point de départ.

4.4.2 Mode voyage

Ce mode est dévolu aux utilisateurs qui se trouvent en voyage, normalement dans une juridiction au-delà de leur pays. Il y est question de traverser des douanes et frontières [403 et 404], de juridictions applicables, de raccordement (« *roaming* ») et de prévention/préparation.

Ce mode **doit** prévoir une minimalisation sécuritaire au moment de traverser les douanes frontière.

Ce mode **doit** permettre de définir la juridiction applicable [186]

Ce mode **doit** permettre de se conformer au droit national applicable

Ce mode **doit** permettre de déclarer le voyage aux tiers concernés (opérateur de plateforme, système de paiement, etc.) afin de prévenir les fausses alertes [405].

Ce mode **doit** permettre de bénéficier du raccordement (« *roaming* »)

Ce mode, lorsque combiné à un mode commandité, **doit** permettre au commanditaire de bénéficier des adaptations nécessaires (ex : cibler la publicité de manière à ne pas avoir les publicités destinées au Québécois au Québec, mais aux Québécois en voyage à l'endroit visité)

Ce mode **doit** permettre de choisir un tiers de confiance [406] en prévision d'une incapacité d'agir, de besoins de représentation consulaire [407] ou en cas de décès à l'étranger [408].

4.4.3 Mode commandité

Le mode commandité en est un où l'utilisateur accepte en toute connaissance de cause de céder une part de contrôle de son utilisation, (par exemple, la collecte de son positionnement GPS) ou l'accès à ses contacts, contre un quelconque avantage, qu'il soit circonscrit au monde virtuel ou qu'il existe dans le monde réel. Ce mode vise à éviter les situations où les utilisateurs fournissent des quantités importantes de données sans aucune contrepartie, voire même en payant pour le service. À ce stade, l'utilisation d'un monétiseur peut être utile puisque les échanges et négociations peuvent être complexes. Ce mode peut, par exemple, permettre d'obtenir des accès VIP à un spectacle ou être activé lorsqu'on passe à la caisse et qu'on paie avec notre application de fidélisation client, laquelle n'a pas besoin de connaître le reste de la journée. Du côté de l'opérateur, ce mode a plusieurs avantages : il s'assure de la coopération et de la véritable participation volontaire de l'utilisateur (ce qui peut augmenter son taux de réponse et d'engagement ou d'adhésion « *conversion rate* ») et surtout, il peut permettre la mise en œuvre de contrats intelligents [382] au renfort de technologies d'informatique de confiance [335] ; bref, s'assurer que l'utilisateur, ayant vraiment consenti de manière volontaire, n'utilise pas de méthodes de protection telles les bloqueurs de publicité [409 et 410] ou les obfuscateurs de positionnement.

Ce mode **doit** informer l'utilisateur de son apport (ce qu'il cède)

Ce mode **doit** présenter un contrat formel, lequel doit être négociable et dont un résumé doit être aisément compréhensible.

Ce mode **doit** être déclaré et rattaché à la couche session

Ce mode **doit** permettre l'utilisation de contrats intelligents

Ce mode **doit** permettre l'utilisation d'un monétiseur

Ce mode **doit** permettre de basculer en mode informatique de confiance.

4.4.4 Mode basculement d'identités

Parfois, les utilisateurs occupent plus d'un rôle à la fois et cela leur amène à avoir une pluralité d'identités, non pas sous des noms différents, mais dictées par leurs appartenances à des groupes multiples. Parfois, il peut être souhaitable que ces appartenances ne se croisent pas, qu'elles soient proprement segmentées. Par exemple, si un employeur permet une politique BYOD, il peut être convenu avec l'utilisateur que l'employeur a une prérogative légitime à surveiller certaines de ces activités. Alors, comment s'assurer qu'il ne dépasse pas et qu'il ne s'immisce pas dans la portion privée des activités sur mobile? La réponse se trouve dans un contrôle de type MAC qui permette d'accéder uniquement au contenu se trouvant sous le contexte ratraché à l'identité de travail. Bien entendu, s'il le désire, il peut bloquer l'accès de l'appareil hors cette identité ou offrir un service très restreint (ex : désactiver le SSL ou l'accès aux fichiers de l'entreprise). Évidemment, la sécurité sous cette perspective ne peut être garantie que si l'identité exige ce mode exclusivement. Dans le cas contraire, cela permettrait une transitivité vers un mode DAC, ce qui constituerait un problème majeur de conception rendant toute politique de sécurité vaine. Bref, ce mode évite d'avoir matériellement un appareil pour chaque identité assumée. Ce mode peut aussi servir dans les cas d'appareils partagés entre plus d'un individu.

Ce mode **doit** permettre aux utilisateurs qui opèrent divers rôles en même temps d'intégrer de manière segmentée leurs identités.

Ce mode **doit** être exclusif pour un appareil ou, lorsque combiné au mode d'agrégation des identités, il doit permettre de séparer les identités voulant être segmentées de celles acceptant d'être agrégées

Ce mode **doit** utiliser un contrôle de type MAC

Ce mode **doit** inclure des règles formalisées de basculement et partages entre identités, lesquelles doivent s'inscrire dans la couche système ou infrastructure.

4.4.5 Mode agrégation d'identités

Parfois, il se peut qu'un utilisateur ne cherche pas à segmenter ses identités, mais au contraire, à les agréger, puisque cela peut être plus facile, rapide ou autrement approprié à sa situation. Dans ce cas, il peut être utile d'offrir cette option et de permettre des agrégations d'identités. Or, ce ne sont pas toutes les identités que l'on veut agréger. On peut vouloir dresser des divisions valables, quoique moins formelles que celles décrites en [S: 4.4.4]. Par exemple, on peut vouloir permettre l'agrégation de toutes nos identités d'étudiant aux diverses universités que l'on fréquente, mais pas celle de nos identités d'emploi.

Ce mode **doit** permettre aux utilisateurs qui opèrent divers rôles en même temps d'intégrer de manière agrégée leurs identités.

Ce mode **doit** inclure des règles formalisées de segmentation et partages entre identités.

4.4.6 Mode discrétion

Ce mode sert une utilité fondamentale à la présente étude et constitue la soupape par laquelle les UFs peuvent exulter leurs faiblesses et autres cachoteries qui font partie de leur identité et de leur humanité. Ce mode doit permettre une action intraçable, qui se veut ponctuelle. Le principal désavantage d'une utilisation touts azimuts de ce mode est pour l'utilisateur, puisqu'il perd toute capacité de mémoire et de continuité. Pour l'État, il s'agit d'un compromis puisqu'il évite de perdre toute capacité de surveillance et le coût est presque nul puisque les clientèles interlopes utilisent déjà des technologies assurant un niveau de protection qui n'est pas inférieur au niveau proposé par ce mode.

Ce mode **doit** permettre une utilisation raisonnablement amnésique [411].

Ce mode **doit** permettre l'accès à des fonctions de cryptographie et permettre d'accéder en lecture et écriture à du contenu crypté.

Ce mode **doit** permettre la navigation obfusquée, tant au niveau réseau, que dans l'obfuscation des opérations au niveau de la couche infrastructure.

4.4.7 Mode propriétaire

Ce mode se situe le plus près du mode « manuel » mentionné au début de la section [S : 4.4]. Or, en contrepartie, il requiert une certaine indépendance en moyens de l'utilisateur. Ainsi, la GIDIM y est fournie par un service indépendant, l'accès Internet est également un produit consommé et, enfin, le contenu est celui pour lequel l'utilisateur a acquis les droits, le tout à ses frais ou libre de droits. Ce mode vise à éviter que le client paie, mais ne contrôle pas. Il est un peu le contraire du mode décrit en [S: 4.4.3]. Le principal désavantage de ce mode, outre l'aspect financier, est la responsabilité finale du propriétaire. Par exemple, il doit s'assurer de la sauvegarde de ses données et en cas de souci, il ne pourra blâmer que lui. Il doit donc disposer de moyens, d'infrastructures, mais aussi d'un certain niveau de connaissances et de discipline. Similairement, s'il est piraté ou qu'il perd sa clé, c'est fini : il ne pourra avoir ni recours, ni secours externes. Ce mode est très compatible avec la philosophie Bitcoin et plus libertaire [412].

Ce mode **doit** offrir le plus grand contrôle possible sur l'appareil à l'utilisateur

Ce mode **doit** être modulaire et pouvoir accéder à la couche système.

Ce mode **doit** permettre l'installation au libre choix de modules et de services de GIDIM auprès du fournisseur retenu par l'utilisateur.

4.4.8 Mode invité

Le prochain mode est tout le contraire et il existe déjà sur plusieurs ordinateurs. Il s'agit d'un mode temporaire généralement minimaliste et permettant d'utiliser, avec sa permission, les ressources d'autrui. Il offre une attente de vie privée [427] réduite et n'offre (à long terme) aucune garantie sur les ressources. Il permet de dépanner un individu de manière sécurisée, par exemple, pour lui permettre de placer un appel. Ce mode, ou un de ses sous-modes, peut être retenu comme configuration par défaut en absence de code d'accès, par exemple, pour permettre à un individu ayant trouvé le téléphone d'appeler son propriétaire [414] ou un tiers de confiance, ou bien encore à tout individu d'appeler les services d'urgence [414]. Une attention particulière doit être portée à l'enjeu d'élévation de privilèges.

Ce mode **doit** déclarer sa qualité de service et ses termes et conditions de manière facilement compréhensible

Ce mode **doit** permettre l'activation de mécanismes de surveillance

Ce mode **doit** permettre l'accès non-restreint aux services d'urgence et au GPS

4.4.9 Mode membre

Ce mode permet non seulement d'utiliser une identité auprès d'un groupe où on est membre (voir [S: 4.4.4]), mais aussi d'appliquer des politiques de déploiement sur l'ensemble de l'appareil et d'être en conformité avec celles-ci. Cela correspond usuellement à un contexte où le propriétaire de l'appareil est un tiers (groupe dont l'UF est membre) et que l'appareil est prêté à l'utilisateur. Ce mode peut permettre le basculement ou l'agrégation d'identités, mais les prérogatives sont inversées du fait qu'il y a une prérogative légitime du propriétaire extérieur à contrôler l'appareil, mais aussi une expectative raisonnable de vie privée de la part de l'utilisateur.

Ce mode **doit** permettre d'opérer selon les objectifs et politiques du groupe

Ce mode **doit** rendre accessibles les termes et conditions, tant lisibles que formalisées, d'utilisation dictées par le groupe.

4.4.10 Mode administrateur et technique

Ce mode vise à opérer les activités techniques sur l'appareil, que celles-ci soient de configuration, d'audit, de débogage, de développement, de test ou de simulation. Il se peut que des applications ou des services refusent de fonctionner sous ce mode et, dépendamment du contexte d'informatique de confiance ou non, il se peut qu'elles soient informées de ce mode, ou pas. Par exemple, le mode administrateur peut permettre de changer, par simulation, sa position géographique et il se peut qu'une application (ex : *Netflix* Canada) n'ait pas intérêt à opérer sous ce mode ou bien qu'elle puisse restreindre ou conditionner l'utilisation sous ce mode (ex : une heure par mois à des fins de configuration). L'idée derrière ce mode est de répondre aux besoins d'opérations exceptionnelles, de manière à les isoler et les centraliser, tout en évitant l'adoption de configurations permanentes offrant ces possibilités, mais encourant plus de risques. Ce mode doit être utilisé pour configurer les modes.

Ce mode **doit** exister sur les appareils.

Ce mode **doit** pouvoir accéder à la couche système.

Ce mode **doit** offrir le plus grand contrôle à l'utilisateur (« *root access* »)

Ce mode **doit** être le seul à permettre les fonctionnalités de configuration système, la définition des permissions, le raccordement à des politiques, le débogage, le développement, les tests, la maintenance et la simulation.

4.4.11 Mode professionnel

Ce mode permet une utilisation dédiée, avec uniquement des identités professionnelles. Il vise surtout à activer les fonctionnalités d'audit. Il peut être recommandé de l'utiliser seul (à des fins de conformité) ou bien, si l'organisme régissant la profession le permet, il peut être combiné à un mode tel que décrit aux sections [S: 4.4.2, 4.4.4, 4.4.9 et 4.4.12]. Il ne peut être combiné aux modes décrits aux points [S:4.4.3, 4.4.5, 4.4.6 et 4.4.7]. Les spécifications relatives à ce mode demeurent à être définies. Ce mode peut voir une pertinence en des méthodes de GIDIM ponctuellement plus sophistiquées, voir invasives.

Ce mode **doit** permettre des fonctionnalités avancées d'audit au niveau session.

Ce mode **doit** être exclusivement déployé seul ou avec des modes compatibles.

4.4.12 Mode sécurisé

Ce mode doit permettre d'accéder à des données particulièrement sensibles et vise à éviter que celles-ci soient accessibles en tout temps. Il vise également à éviter qu'elles soient accessibles au travers des usurpations du mode utilisateur. Ce mode offre un caractère plus solennel et officiel, lequel peut être nécessaire ponctuellement, par exemple, lors d'utilisations de technologies financières (ex : paiement et transactions) ou civiques (ex : élections électroniques, interactions avec l'État), ainsi que lorsqu'un service de GIDIM nous désigne comme tiers de confiance. Ce mode aussi peut voir une pertinence en des méthodes de GIDIM ponctuellement plus sophistiquées, voir invasives, telles la biométrie.

Ce mode **doit** être réservé à des opérations ponctuelles nécessitant un contexte sécuritaire particulier

Ce mode **doit** pouvoir utiliser des méthodes d'authentification et de GIDIM, telles celles faisant usage de la biométrie

Ce mode **doit** faire usage de réseaux de propositions

4.4.13 Mode portable

Si on pousse le concept de virtualisation et de modularisation au bout du raisonnement, on se rend compte que l'appareil mobile n'est qu'un point de contact et que les politiques relatives à l'appareil sont possiblement peu importantes, ce qui importe, c'est ce qui est fait par l'appareil. Une telle perspective permet notamment d'abstraire le concept de point de contact, lequel n'a plus besoin d'être ni final, ni unique. Par exemple, en matière d'Internet des Objets, le point de contact peut être un objet connecté ou l'appareil mobile qui les orchestre, du fait que celui-ci a une interface plus complète. Similairement, la GIDIM peut s'étendre à une automobile ou à un vêtement intelligent. Cette approche quitte l'informatique personnelle où le point de contact est usuellement la propriété de l'individu et transitionne vers une conception de point de contact public ou point temporaire. Le mode correspondant peut donc permettre d'employer l'appareil comme une coquille vide et sa GIDIM modulaire permet de solliciter, puis d'accéder à des identités téléchargées auprès d'un fournisseur ou un médium au niveau de la couche session.

Ce mode **doit** offrir des conteneurs sécurisés et cryptés pour chaque identité au niveau infrastructure et, si possible, au niveau système

Ce mode **doit** permettre le chargement (par réseau ou médium) de politiques à être déployées au niveau infrastructure.

Ce mode **doit** inclure une approche modulaire de GIDIM permettant le chargement (par réseau ou par médium) des identités.

4.5 Activité de gestion : gestion et transition entre les modes

Transitions entre les modes

Maintenant que les principaux modes retenus ont été présentés, il peut être pertinent d'aborder la question des transitions entre ces divers modes, lorsque plus d'un mode réside sur un même appareil.

4.5.1 Transitions triviales

Certaines de ces transitions seront triviales, d'autres impossibles. Par exemple, le mode professionnel et le mode commandité sont incompatibles alors que de basculer entre un mode propriétaire et un mode invité ou discrétion peut se faire d'un simple clic. Pour ces modes, la simplicité de transition doit être encouragée.

4.5.2 Transitions avec compensation économique

Il se peut cependant que des transitions puissent être plus complexes. Par exemple, la transition entre un mode membre ou un mode commandité vers un mode propriétaire requiert un changement de nature économique. Le cas échéant, la possibilité doit être offerte, ainsi que celle d'offrir une compensation. La méthode proposée pour ces transitions est d'une formulation de demande de transition formalisée sur laquelle les parties prenantes intéressées pourront poser leur signature ayant valeur d'autorisation.

Gestion des rôles

4.5.3 Classement des rôles et leur gestion

Les divers modèles, ainsi que les rôles peuvent faire l'objet d'opérations intellectuelles d'étude, d'analyse, de classement et de gestion. Par exemple, il peut être utile de proposer une catégorisation qui permette de segmenter les modes qui sont compatibles entre eux ainsi que les conditions de cette compatibilité.

4.5.4 Analyse des écarts, de leurs causes et de leurs conséquences

Malgré ces efforts, des écarts vont subsister et ceux-ci auront des conséquences qu'il serait pertinent d'étudier, mais cela sera réservé à des itérations ultérieures du processus de recherche.

Association des modes

Tableau 4.6 – Association des modes et des clientèles (4.5.5)

#	Mode	Clientèles									
		Utilisateurs personnels	Utilisateurs professionnels légitimes	Individus vulnérables et sous assistance	Représentants politiques	Uutilisateurs techniques de service	Utilisateurs , interlopes	Utilisateurs académiques	Utilisateurs de surveillance et d'audit	Utilisateurs atypiques	Migrants
01	Ordinaire	-	-	-	-	-	-	-	-	-	-
02	Voyage	Q	Q	N	Q	N	Q	Q	Q	Q	**Q**
03	Commandité	Q	N	**Q**	N	N	N	Q	N	Q	Q
04	Basculement	Q	Q	N	Q	Q	Q	Q	Q	**Q**	Q
05	Agrégation	**Q**	Q	Q	N	Q	N	Q	N	Q	Q
06	Discrétion	Q	N	Q	Q	Q	**Q**	Q	Q	Q	Q
07	Propriétaire	Q	Q	Q	Q	Q	Q	Q	Q	Q	Q
08	Invité	Q	N	Q	N	N	Q	Q	N	Q	Q
09	Membre	Q	Q	Q	Q	Q	Q	**Q**	Q	Q	N
10	Admin. & tech.	N	Q	Q	N	**Q**	N	Q	Q	Q	N
11	Professionnel	N	**Q**	Q	Q	Q	N	Q	**Q**	Q	N
12	Sécurisé	Q	Q	Q	**Q**	Q	Q	Q	Q	Q	Q
13	Portable	Q	Q	Q	Q	Q	Q	Q	Q	Q	Q

Q : Ce mode satisfait à au moins quelques besoins particuliers à cette clientèle

N : Ce mode ne satisfait pas à des besoins particuliers de ce groupe

- : Sans objet; Gras : meilleur mode recommandé

Tableau 4.7 – Association des modes et des modèles d'affaires (4.5.6)

# **Mode**	Modèles d'affaires: Vente d'appareils	Vente de licences individuelles	Vente de publicité	Vente de services
01 Ordinaire	x	x	x	x
02 Voyage			x	x
03 Commandité			x	
04 Basculement		x	x	x
05 Agrégation				x
06 Discrétion	x			x
07 Propriétaire	x	x		x
08 Invité				
09 Membre		x		
10 Admin. & tech.	x			x
11 Professionnel	x	x		x
12 Sécurisé				x
13 Portable			x	x

x : Compatibilité claire du mode avec le modèle d'affaires

4.6 Autres observations spécifiques aux principales plateformes (projections)

Face à l'avenir les deux plateformes semblent suivre des évolutions fort différentes et il peut être à propos d'en brosser les grandes lignes.

4.6.1 *Apple* et son évolution tels qu'observées

Apple semble suivre un cours immuable où, à coup d'énormes moyens, elle enrichit une offre basée sur un modèle d'affaires assez inchangé en plus de dix (10) ans. Suite au cas de San Bernardino [413 et 428], *Apple* a quelque peu changé son positionnement et semble s'orienter vers un modèle plus compatible avec le « mode propriétaire », sous de nombreuses restrictions. Le problème fondamental avec cette approche est que tant que les entreprises seront des créatures soumises au droit national, voire extranational [186], elles ne pourront s'abstenir de leur devoir de communiquer aux États les informations exigées par mandat judiciaire.

4.6.2 *Android* et son évolution tels qu'observés

Android, quant à lui, a le défaut de ses qualités. L'offre d'*Android* étant gratuite et grandement basée sur le logiciel libre, c'est la concurrence par les petits joueurs qui présente le principal risque. De plus, comme les entreprises et les individus vivent avec les conséquences de leurs décisions, la part de marché importante qu'occupe Samsung dans la fabrication d'appareils lui confère une influence importante. Le fait prévisible qu'il s'agisse d'une entreprise d'un pays émergeant semble faire poindre de possibles discordes géopolitiques et c'est ce qui justifie le développement de plateformes sinophiles.

4.7 Extensions proposées et leur justification

Outre les modes d'opération, il y a quelques autres apports qui sont proposés. Bien que dans l'absolu, seule l'imagination puisse être la limite, en pratique il sera pertinent de se limiter à un ensemble très restreint d'innovations pouvant être utilisées de pair avec les modes. Ces extensions visent une évolution dans le temps, tant au niveau du développement des technologies que de son adoption par toutes les parties prenantes. À cet égard, celles retenues sont les suivantes:

4.7.1 Témoins matériels directs (permettant de connaître le mode employé)

Le principal besoin dans lequel s'inscrit cette extension proposée est celui du composant de l'intégrité dans le besoin de sécurité. Il faut que l'UF puisse avoir un degré de confiance raisonnable à l'effet que l'appareil fonctionne de manière conforme et prévisible à ce à quoi il s'attend, ce qui inclut que son état ne puisse être facilement falsifié. Cela permet notamment à l'utilisateur d'avoir une idée la plus fiable possible, de quand son appareil peut être compromis. À ce chapitre, notons que la plupart des compromissions, auprès de la plupart des UFs relèvent de la cybercriminalité et non de la surveillance policière ou d'État. Par conséquent, un tel indicateur a sa raison d'être ajouté, au vu des besoins des utilisateurs. Il permet notamment à l'utilisateur d'adopter un comportement adéquat face à l'état dans lequel se trouve son appareil.

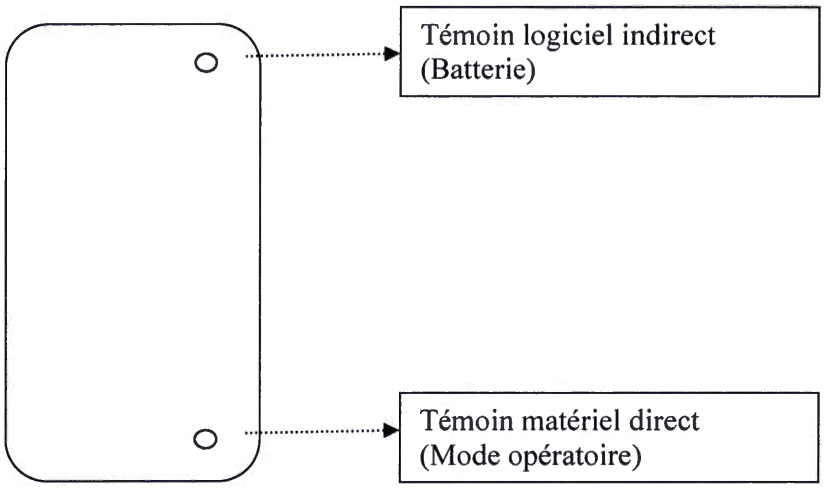


Figure 4.1 – Exemple de mise en œuvre de témoin matériel direct

4.7.2 Stratégies de segmentation anti-collusion (permettant d'éviter que les OPs, ou autres, ne subvertissent les modes).

Dans une livraison de services de plus en plus dématérialisée, le contrôle physique sur les ressources de stockage ou de traitement cède sa place aux stratégies d'informatique distribuée et ces stratégies peuvent être distribuées, non seulement au chapitre de l'extensibilité des ressources, mais aussi de leur dispersion géographique, voire même des parties impliquées dans ce processus de distribution. Évidemment, cela amène toute la question de l'extra-territorialité des lois, en particulier au vu du développement que vient de produire la Cour Suprême du Canada sur la question (arrêt Google Inc. c. Equustek Solutions Inc.[186]). Parfois, il peut y avoir des conflits entre les impératifs légaux auxquels un opérateur peut être soumis et il faut aussi comprendre qu'un territoire étranger n'a pas d'autres incitatif, outre de développer son offre de service à l'international, de protéger les citoyens des autres États comme il le ferait avec ses propres citoyens. Aussi, avec l'arrivée des contrats intelligents, il se peut que les fournisseurs d'accès en nuage ne soient que des revendeurs et que, au bout du compte, l'opération de calcul, de communication ou de

stockage soit offerte via une enchère automatisée. Dans tous les cas favorisant la libre concurrence, le risque de collusion risque de poindre parce que la concurrence, en absence de mesures visant à l'assurer, peut pâtir de la concentration inhéremment oligopolistique de ressources ainsi que des intérêts et aléas de chaque partie prenante.

Cette extension revêt une importance accrue au regard des besoins en matière de couverture des régions isolées et rurales ainsi qu'en matière de diversité de l'offre. Ils visent à assurer un niveau d'indépendance garanti peu importe qui offre les services et, éventuellement, des concentrations ou fusions entre OPs, OAS et/ou OTs.

Enfin, sous un aspect géopolitique, cela permet aussi d'assurer le besoin de souveraineté technologique, en ne permettant pas de reproduire divers processus conflictuels tels les embargos et blocus.

4.7.3 Assistant virtuel représente l'aboutissement de la réflexion et de la mise en œuvre du souci de voir s'exprimer (et primer) les besoins des UFs.

L'assistant privé virtuel est probablement l'extension la plus prometteuse à côté des modes opératoires. Si on considère que les interactions entre individus ainsi qu'entre ces individus et les autres parties prenantes se complexifient, cette voie peut être la seule disponible dans un horizon qui pourrait se qualifier comme relevant du moyen-terme. Ce serait une solution systémique à un problème systémique, pourvu que cet assistant ait comme seule priorité l'intérêt de l'UF. Cela permettrait notamment de répondre au besoin de minimiser, à la source, la collecte et la transmission d'informations personnelles, surtout s'il est possible d'utiliser cet assistant comme tiers de confiance ou entité fédérée à des fins de GIDIM.

En ce qui concerne le besoin d'importance, celui-ci est comblé par cette extension du fait que l'utilisateur entre dans une négociation plus horizontale, du moins en principe, quant à l'importance qu'il est prêt à accorder à ses données.

Enfin, en ce qui concerne la temporalité, un assistant virtuel automatisé pourrait s'adonner à des activités de veille afin de s'assurer que les données soient retirées à leur expiration, ce qui est un processus long, méthodique, fastidieux et chronophage, autant de caractéristiques desquelles les UFs seraient grés d'être libérés.

Les principales difficultés inhérentes au développement des technologies d'assistant virtuel qui paraissent évidentes semblent converger vers la difficulté de formaliser les goûts et préférences de l'utilisateur et vers le développement de stratégies de négociation. La première partie de cette considération ramène à la difficulté dans l'essence même de la définition de l'identité dans un environnement numérique.

À terme, encore une fois, il demeure à craindre qu'une iniquité des ressources puisse être exacerbée par une iniquité des assistants.

4.7.4 L'identité portable semble la mise en œuvre la plus imminente au regard des développements récents.

En considérant les développements des technologies de conteneurs ainsi que l'accroissement des vitesses de débit cellulaire, c'est l'identité portable qui semble constituer le prochain jalon dans l'évolution de la GIDIM. Le principal obstacle, à ce jour, à l'adoption de cette technologie est que le coût en bande passant qui est requis ne semble aucunement être compensé par les avantages en contrôle des données par les UFs. Ce déséquilibre est dynamique et évolue en faveur de l'identité mobile au fur et à mesure que les opérations informatiques qui y sont nécessaires se rapprochent d'un coût nul.

4.8 Validation des résultats

Notons d'abord qu'il existe dans le processus une étape qui permet de valider les modes obtenus par rapport aux modèles d'affaires et que celle-ci opère la principale activité de validation de résultats au niveau unitaire.

Or, il serait à propos de rajouter une étape pour valider les résultats au niveau de leur ensemble, téléologiquement.

En l'espèce, il s'agit d'un bref recensement de diverses initiatives logicielles qui tentent, au mieux, de répondre aux besoins identifiés, mais par « le dessus » (« *top down* »), le plus souvent au niveau applicatif plutôt que d'enchasser correctement ces fonctionnalités au niveau système, ce qui constitue justement le changement que l'on tente de justifier.

(4.8.1) Mode ordinaire (par défaut)

Sans objet

(4.8.2) Mode voyage

Fonctionnalité de déni possible (« *plausible deniability* ») dédiée au franchissement de frontières dans l'application ESCrypt sous *Android.*

Rien sous Àpple.

(4.8.3) Mode commandité

Plateforme *AdMob* rachetée par Google

Fonction « *interest-based ads* » de l'*AppStore* et de l'application enchâssée « Nouvelles » sous *Apple.*

(4.8.4) Mode basculement d'identités

Sans objet spécifiquement, quoique la multiplicité des adresses et comptes courriel joue, *de facto*, ce rôle, tant sous *iOS* que sous *Android.*

(4.8.5) Mode agrégation d'identités

Application « *Identity* » sous *Android*

Sans objet sous *Apple*, quoique l'appli *Simplikity*, et autres gestionnaires de mots de passe, vont dans ce sens.

(4.8.6) Mode discrétion

Fonctions « Vie privée » ou « Incognito » de diverses applications, principalement Firefox, Opera, Safari et Chrome, sous les deux plateformes.

(4.8.7) Mode propriétaire

Sans objet au niveau des applications. Or, les phénomènes de la popularité du *jailbreaking* et du *rooting* militent en ce sens.

(4.8.8) Mode invité

Sans objet

(4.8.9) Mode membre

Applications *McGraw Hill* (*Education*)

(4.8.10) Mode administrateur et technique

Xamarin testcloud

(4.8.11) Mode professionnel

Sans objet

(4.8.12) Mode sécurisé

Fonctionnalités identification multifacteur (*FB*, *GoDaddy*, etc.)

(4.8.13) Mode portable

Fonctionnalité Pocket de Firefox

() : Les parenthèses indiquent un emprunt-calque de la section 4.4 et sous-sections.

4.9 Distinction entre Knox et le modèle proposé

Le modèle proposé se distingue de celui offert par Knox du fait qu'il en est la généralisation. Le système Knox pose les premiers jalons de l'utilisation de conteneurs, mais le fait d'une manière qui se limite un peu au mode décrit par [S: 4.4.5]. Cela reflète le fait de suivre les besoins en matière de BYOD, principalement basés sur les besoins des entreprises et non des individus.

La présente étude permet de constater que Knox est un pas dans la bonne direction du fait qu'il y a une certaine amélioration. À la base, le fait de remettre en cause le mode opératoire unique est une étape déterminante. Il ouvre la porte de ce qui devient ainsi variable et ensuite, l'évolution se façonne au gré de la capacité des diverses options disponibles à répondre adéquatement aux besoins. Plusieurs options sont possibles.

À l'heure actuelle, la technologie Knox est déjà rendue à sa version 2.0 et elle continue d'évoluer. Il s'agit d'un train en marche, voire de vive allure; apparaissent donc les difficultés particulières que l'on peut imaginer à ce contexte quant à la mise en contraste entre les caractéristiques de Knox et le modèle proposé. Il est donc important de considérer, surtout au regard d'éventuelles inclusions indépendantes d'améliorations proposées, de l'état de la situation au moment de l'étude.

Ces distinctions actuelles se résument donc en quelques points. Avant tout, Knox est une amélioration purement logicielle, alors que l'ensemble des extensions proposées incluent des volets matériels. Or, cela ne devrait pas poser de grands problèmes puisque Samsung est également constructeur de matériel. Ensuite, Knox est orienté emploi. Parmi les grands chambardements mentionnés plus haut, il ne faut pas perdre de vue la transformation de la réalité du travail, rendant de plus en plus rare la formule d'emploi typique et favorisant le travail autonome. À ce chapitre, la philosophie derrière Knox est différente de celle à partir de laquelle le modèle de changements proposés a été développée puisque cette dernière vise à répondre à un vaste éventail de rôles et configurations. Si le travail change, il se peut que les études changent, mais aussi la perception de bénéfices sociaux. Ainsi, la diversité des avenues contemplées est plus large avec l'option retenue qu'avec Knox. Enfin,

fondamentalement, la principale différence conceptuelle réside dans le fait que, dans le modèle proposé, c'est l'UF qui est aux commandes; la conception vise à refléter ses besoins de manière prioritaire. Cela requiert notamment que ces besoins puissent, selon la volonté de l'UF, pouvoir être intégrés à ceux des autres parties prenantes.

4.10 Ouverture et discussions

À la lumière des résultats obtenus, il est clair qu'il est possible de théoriser au sujet des besoins des utilisateurs et d'en dégager des besoins qui pourront ensuite devenir des exigences, malgré le caractère disparate, voire contradictoires des besoins exprimés par la variété des types et clientèles d'UFs. Les modes d'opération permettent donc d'organiser l'utilisation des appareils mobiles sous des cas types, qu'il faudrait peut-être ensuite formaliser davantage.

C'est donc vers son terme que la présente étude se dirige, mais tout tel terme peut déboucher sur d'autres ouvertures du fait que les réponses trouvées suscitent souvent les questions qui seront la base des travaux qui suivront. Il est alors à propos de faire le bilan de l'activité de recherche, ce qui se fait en quatre temps et deux sections. D'abord, il est de mise d'exprimer les questions et observations qui deviennent, à l'occasion de cet aboutissement, les candidates les plus pertinentes pour guider les efforts de recherche subséquents. Ensuite, il faut revenir sur ce qui a été accompli. Dans une deuxième phase, la conclusion, il faut inscrire les résultats dans le temps et présenter des réflexions sur les évolutions possibles du phénomène étudié. Si tout cela demeure bien aligné, les étapes subséquentes pourraient se raccorder à la suite et dans la continuité de ce qui a été fait, ou alors, dans le cas contraire, s'inscrire dans une stratégie différente, si les conclusions dictent que c'est ce qu'il faut faire, ce qui est par exemple le cas lorsque les résultats ne sont pas concluants ou que l'on remarque qu'il y a un problème dans la démarche.

Heureusement, la présente étude ne semble pas souffrir d'un tel aboutissement. Le fait qu'il s'agisse d'un travail exploratoire et descriptif aide beaucoup à la viabilité du résultat. En l'espèce, le résultat est un modèle évolutif, mais riche d'améliorations à apporter au-delà de Knox et il semble présenter une avenue intéressante et viable de changements qui

sont à la fois pertinents et réalisables (parce que finançables). Ce dernier point demeure d'une grande importance puisqu'il ne faut pas oublier que la démarche visait à s'inscrire dans un processus de GL, exposé aux contraintes du monde réel, et non dans un cadre purement théorique. Dans celui-ci, après l'analyse des besoins, les divers corpus disciplinaires présentent les autres étapes du développement. Attendu que le but visé était de représenter les besoins des UFs alors que ceux-ci ne présentent pas un groupe sondable puisqu'il s'agit d'une population au sens politique, les principaux risques qui auraient pu faire dérailler la présente étude et ses objectifs de recherche s'articulaient autour des courants d'intérêts au sein de cette population et des tensions entre ceux-ci. Des polarisations, des effets de grappe ou bien des tensions auraient pu rendre la présente étude impraticable ou ses résultats peu exp loitables. Par exemple, le développement d'applications « de rencontre » hétérosexuelles présentent des groupements par sexe avec des besoins relatifs à l'application qui sont possiblement bien différents entre ces deux groupes, et bien marqués : un tel exercice d'élicitation des besoins aurait été confronté à cette particularité. Similairement, une application transactionnelle regroupant des marchands et des clients connaît des défis similaires.

4.10.1 Ouvertures de recherche

Si on choisit de poursuivre la voie des raisonnements employés au cours de la présente étude, plusieurs étapes pourraient suivre, dont la définition formelle des modes ainsi que de leurs mécanismes de gestion et de transition. L'ensemble de ces construits pourront être testés pour qu'en soit mesurée qualitativement, puis quantitativement leur pertinence et éventuellement, cela mènera à des optimisations.

À ce chapitre, les principales ouvertures possibles concernent les étapes suivant l'élaboration d'exigences, puis de devis et d'artéfacts de conception devant mener à la mise en œuvre de la solution logicielle ou des changements qui sont visés. Pour raccorder avec ces étapes ultérieures, il faudrait probablement ordonner les besoins exprimés et dresser un portrait plus détaillé des segments de la population pour lesquels on vise à apporter une amélioration. Ensuite, une fois qu'on a une image plus claire, la prochaine étape serait de tenter d'identifier des écarts entre les besoins exprimés dans la littérature consultée et la

réalité actuelle. Ces écarts peuvent avoir comme cause la durée de l'étude, le hasard, les biais ainsi que tous les autres facteurs qui contribuent normalement à ce que la réalité diffère légèrement de la théorie. Pour combler ces écarts, une démarche proposée serait de bâtir des cas d'utilisation plus formellement et de les soumettre pour validation. Dépendamment de la stratégie et du cycle de développement, cette validation peut avoir lieu au travers de groupes de discussion (« *focus groups* ») ou bien par des études de cas ou l'instrumentation et l'interaction avec la communauté des utilisateurs (« *community feedback* »). Si les moyens le permettent, un groupe pourrait être exposé à un prototype minimal fonctionnel ou bien, si les moyens sont plus importants, des déploiements contrôlés de petits lots d'appareils améliorés pourraient être distribuées afin d'étudier l'adoption des nouvelles fonctionnalités par les UFs. Enfin, ce qui limite le processus de génie logiciel dans les circonstances, c'est essentiellement l'absence d'un interlocuteur représentatif. Amener les citoyens à s'impliquer, à participer activement au développement de la réalité informatique qui les entoure est une avenue sociétale qui règlerait le même déficit que la présente étude tente de combler de manière technique, par la gestion et le génie logiciel. Au regard de la présente étude, un tel changement sociétal serait de nature à contribuer à la satisfaction des objectifs à long-terme dans lesquels la présente étude s'inscrit. La participation des UFs dans le processus de développement est une réalité assez nouvelle et elle aussi mérite des recherches, notamment sur les facteurs favorisant de telles implications de la part des citoyens.

4.10.2 Discussions

Dès le départ, la présente étude s'est attaquée à une problématique fort complexe, principalement de par son interdisciplinarité, mais plus fondamentalement, de par le facteur humain qu'elle intègre, lequel ouvre des pans politiques et sociologiques desquels il a fallu se garder pour se concentrer sur les aspects techniques, tout en gardant à l'esprit leur proximité. Fondamentalement, le développement de technologies suit, dans l'Histoire, une évolution turbulente puisqu'elle bouscule bien des choses, dont les rapports de pouvoir. Il est donc normal qu'il y ait une période où les besoins ne soient pas dictés selon les meilleures pratiques du génie (logiciel), lequel présente une évolution ordonnée, mais

plutôt selon les préoccupations de ceux qui ont les moyens de mener ce développement. Tout aussi naturellement, dans la durée, ces écarts se comblent soit par le besoin de demeurer actuel ressentis par les OPs, soit par des prises de contrôle plus directes, individuelles ou collectives. Dans un cas comme dans l'autre, disposer d'une connaissance structurée qui puisse servir de point de départ à cette conciliation semble être d'une valeur tant académique que sociale et technique.

La littérature consultée illustre une situation où il y a des divergences claires et affirmées, et les besoins peuvent être inconciliables un à un, mais les rapports entre les différentes parties de la population permettent le dialogue constructif. Ce n'est malheureusement pas toujours le cas. L'histoire en matière de GIDI montre que des tensions bien plus vives peuvent être observées, ce qui rend impraticable un exercice comme celui qui vient de se conclure. Par exemple, sous le régime de Vichy, la situation aurait été incomparable puisque les enjeux de surveillance d'État n'auraient pas permis une discussion aussi paisible. Similairement, il existe encore de nos jours des pays où un tel dialogue ne peut pas avoir lieu. Cela met de l'avant le caractère circonscrit dans l'espace et dans le temps, ou dans le mode de vie social, de ce phénomène. Il ya un constat qui semble incontesté et c'est celui à l'effet que le changement ne pourra pas venir du fait d'un seul individu, ni de l'individu seul. Il faut donc décider quelle véhicule de changement sera retenu pour matérialiser ces changements proposés ainsi que, plus largement, il faudra aussi décider par quels moyens les UFs seront appelés à apporter leur voix au chapitre des caractéristiques des logiciels qu'ils utilisent. Il est aussi envisageable que d'autres formes de communautés ou de collectivités apparaissent telles des communautés d'intérêt, dans le but d'influencer le développement technologique de manière plus conforme à des segments mobilisés de la population. À ce chapitre, de tels segments disposant de moyens de mobilisation importants pourraient être celui des baby-boomers. Il est envisageable que le vieillissement et la péréclitation des facultés qui l'accompagne soient de nature à rendre urgente l'intégration de certaines exigences, telles l'adaptation des technologies aux réalités des UFs aînés, par exemple au travers de modes de GIDIM favorisant l'assistance (mode membre).

4.10.3 Retour

À ce stade, il peut être pertinent d'effectuer un retour sur la démarche de recherche afin de valider si celle-ci s'est déroulée conformément à ce qui était prévu, si on a réussi à dégager cette connaissance recherchée. Sans prétention, la présente étude ne soutient pas d'avoir réglé une question définitivement, ni d'avoir redressé une injustice, loin s'en faut. Or, elle visait à poser un premier jalon le long de l'avenue prometteuse d'un raisonnement cherchant à justifier une plus grande prise en compte des besoins des utilisateurs, aussi divers et variés qu'ils puissent être. Donc, un retour sur la démarche permettrait de constater si l'étude a ou non, été concluante. Pour ce faire, il faut simplement comparer la situation avant la recherche et celle après celle-ci.

Le retour sur la recherche permet également de rendre compte des difficultés rencontrées ainsi que des écueils, de manière à rendre ce parcours intellectuel et opérationnel plus praticable.

Situation avant la recherche

D'abord, la situation avant la recherche (2005) ne portait pas sur les téléphones mobiles, mais sur la GIDI, les téléphones intelligents n'étant pas encore dans le paysage. Ensuite, au fil des évolutions, l'étude s'est centrée autour de la GIDIM et, plus particulièrement des évolutions à proposer afin d'intégrer les besoins des individus en matière de conception des solutions de GIDIM. Tout au long de ces douze (12) années, il est incroyable de voir que les problématiques auxquelles sont confrontées les diverses parties prenantes aient évolué si peu (à l'exception des « *MDM* »), mais il est encourageant de voir que les problématiques essentielles aient été reconnues et étudiées, voire formalisées dans des normes. De nos jours, au fur et à mesure que l'informatique mobile représente une part croissante de l'informatique, il y a un constat à l'effet qu'il y a un plusieurs problèmes en matière de GIDI(M) : le nombre de mots de passe qu'un utilisateur doit retenir explose et demeure lié au nombre de systèmes avec lesquels il doit interagir, cela sonde les limites de la GIDIM manuelle; les débordements des GAFA inquiètent et l'adhésion à leurs services

est vue comme une fatalité. Enfin, au risque de se répéter, les besoins des utilisateurs sont évacués de la conception des systèmes de GIDI(M). Avant d'entamer la présente mouture de l'étude, un recensement approfondi de la littérature n'a pas permis de trouver un travail proposant des moyens de rendre la GIDIM plus représentative des besoins des utilisateurs et ce vide semblait, à l'auteur de la présente, trop désolant pour qu'il reste ainsi.

Situation après la recherche

L'effort de recherche est toujours mu par un effort conscient de chercher à combler un vide, à rassasier une insatisfaction et, en l'espèce, la présente étude est la première à offrir une voie de développement, parmi toutes celles possibles et pertinentes, qui soit capable de répondre à des besoins multiples issus d'une clientèle variée.

La principale difficulté rencontrée a été la focalisation dans le cadre d'un travail académique de type « *mémoire de maîtrise* ». Le sujet étant vaste, il était facile de digresser et les limites étant floues, il était a fallu cerner un seul sujet et y apporter un traitement méthodologique défini.

4.10.4 Rétrospective

Rétrospectivement, s'il y avait des choses à changer dans la présente étude, ce serait d'en modifier un peu la portée afin d'inclure notamment le développement de certains autres plateformes, notamment Tizen et Mer ainsi que les autres qui doivent leur popularité au refus de céder à une vision centrée sur le contexte Nord-Américain. Il y a un nombre important de développements qui se passent outre-mer et qui sont peu documentés en anglais, davantage en cantonais ou coréen.

Un élément à souligner de manière rétrospective est que, sans trop y faire attention, les conclusions de la présente étude peuvent être généralisées. En fait, la problématique de l'absence de voix au chapitre des besoins des UFs dans le génie logiciel existe depuis avant le développement de téléphones intelligents et d'appareils d'informatique mobile. Elle

concerne l'ensemble des logiciels « prêt à rouler », ou « *shelf* » (tablette), développés *in absentia* (des UFs). Il y a cependant une distinction importante et c'est que le caractère hautement personnel des technologies mobiles a offert un contexte mettant en emphase de manière remarquable cette problématique, d'autant plus dans un environnement où il existe des options à code source ouvert où il est possible d'apporter des changements à la situation actuelle.

4.10.5 Perspective future et améliorations possibles

Certains concepts effleurés par la présente étude pourraient être appelés à connaître, dans un horizon inconnu, une adoption considérable. Parmi ceux-ci, figurent probablement le concept d'assistant virtuel ainsi que de technologies civiques, menant éventuellement à la notion de citoyenneté et droits électroniques et peut-être même éventuellement à la citoyenneté en tant que service où chacun pourrait être citoyen du groupe ou pays avec qui il accepte de conclure une entente à cet égard, peu importe où il se trouve dans le monde. Cela peut sembler lointain et étranger comme conception, mais il faut constater que l'État-nation est un concept qui subit une attaque frontale par l'actualité et cela depuis plusieurs décennies maintenant.

Il n'y a aucun moyen de savoir si la marche de l'Histoire empruntera l'avenue pavée par l'humble connaissance qui vient d'être dégagée, seul le temps le dira. Or, au-delà de l'activité neutre de recherche, l'Académie porte aussi comme particularité qu'elle est un vaste espace d'échange d'idées et de préservation historique. Le fait de promouvoir, en la soumettant au regard des pairs, une idée, aide à son amélioration et à sa diffusion. Il existe notamment des ponts permettant de raccorder des activités de recherche comme la présente à des activités de développement, surtout auprès de plateformes de développement comme celles de Mer. Ce serait peut-être un bon point pour diffuser les travaux actuels.

Un projet d'ingénierie s'inscrit usuellement dans la gestion d'un cycle de vie. Ce cycle de vie est généralement proportionnel à la durée de vie du produit. En l'espèce, le produit est le logiciel servant de plateforme d'exploitation des technologies mobiles. Ce créneau est en croissance, de plus en plus d'objets deviennent connectés, plusieurs sont dotées d'interfaces

pour les utilisateurs, d'autres non. Les facteurs susceptibles de ce limiter la vie du logiciel relèvent davantage de chambardements majeurs ou d'évolutions technologiques rendant l'informatique mobile caduque. On peut donc raisonnablement conclure que les questions soulevées par la présente étude demeureront d'actualité pour un certain temps encore. De plus, elles répondent aussi à des questions qui pourront être soulevées ultérieurement, au fur et à mesure que ces technologies seront développées.

Il existe néanmoins des avenues et des *scenarii* qui exigeraient de reconsidérer la présente étude. Par exemple, avec le développement de technologies quantiques, malgré les efforts de développement d'algorithmes cryptographiques post-quantiques, il demeure possible d'entrevoir un avenir matériel, technique et social où plus rien ne serait secret sur les plateformes informatiques. Une telle société de transparence aurait forcément d'autres enjeux et, par conséquent, d'autres besoins. Toujours dans les cas limite, l'automatisation du travail permet de penser éventuellement l'avènement d'une société où le travail serait minimal et où la survie de tous et chacun dépendrait davantage de la redistribution des richesses par l'État que du travail individuel. Un tel changement pourrait changer les rapports d'équilibre quant à nombre de préceptes que l'on assume comme valables du fait de l'hypothèse de mérite individuel et de liberté individuelle. Ces hypothèses pourraient se trouver compromises par de tels changements. Enfin, le développement de technologies de plus en plus invasives pourraient flouter les frontières entre le soi et la machine, ce qui aurait un impact direct sur la notion d'identité. Encore une fois, il faudrait alors reprendre l'étude à la lumière de ces éventuelles évolutions.

Quant à Knox spécifiquement, il y a plusieurs évolutions possibles qui seront probablement déterminées par le marché et les caractéristiques de ses principaux groupes d'utilisateurs. Il se peut que dans un avenir rapproché, talonné par la concurrence, les principales branches de développement d'*Android* finissent par intégrer des fonctionnalités de *Knox* à même le système et peut-être aussi des extensions souhaitables mentionnées par la présente étude. Il se peut aussi que *Knox* demeure une plateforme servant à un créneau spécifique, soit la conciliation de deux rôles : employé et individu. Dans un tel cas, il se peut que Samsung développe une plateforme plus générale servant à répondre aux besoins d'un autre segment de marché, peut-être plus large et général, voire plus ludique. Il est aussi possible qu'un

autre visionnaire arrive à la barre d'*Apple* et que, comme Steve Jobs, il brasse intégralement les cartes.

Il est possible que d'autres avenues qui n'ont pas été envisagées soient celles par lesquelles le parcours de l'Histoire déambulera. Il se peut aussi que de grands chambardements bouleversent nos civilisations et que les besoins des utilisateurs en matière de GIDIM deviennent le cadet des soucis, même pour la communauté académique.

Ayant en vue toutes ces possibilités, la présente étude ne vise qu'à identifier des éléments importants et à documenter les distances entre l'état le plus avancé de la mise en œuvre dans cette direction, *Knox* ayant été repéré à ce titre, et le modèle proposé.

4.10.6 Retour sur les objectifs, la question de recherche et les hypothèses

Les objectifs ayant été posés comme visant l'élaboration d'un modèle de modes d'opération réduisant l'écart entre le modèle de besoins et les modes d'opération existants, il appert que c'est la section [S : 4.5. 5 (et aussi 4.5.6)] qui permettent de conclure que cet objectif a été atteint. En ce qui concerne l'hypothèse de recherche, elle théorisait au sujet de la capacité de trouver, dans la littérature, des besoins pouvant être organisés en modes et que ces modes seraient compatibles avec des modèles d'affaires. Les trois éléments de cette hypothèse semblent satisfaits, il est donc proposé de confirmer l'hypothèse.

4.10.7 Suites spécifiques

À la lumière des résultats obtenus, l'auteur de la présente recommande que les activités d'élaboration de modèles soient remplacées par des activités d'évaluation de modèles et de veille des besoins.

Il est généralement assez risqué de se livrer à des pronostics, mais un peu moins risqué d'identifier des suites spécifiques. En l'espèce, l'évolution générale du phénomène tend vers une maturation des technologies mobiles et une suite spécifique à anticiper serait le

morcèlement partiel, mais croissant de l'oligopole par une multitude de petits concurrents spécialisés visant à reprendre le processus d'élicitation des besoins, mais au compte de petits segments et groupes d'UFs partageant des caractéristiques communes (ex : travailleurs autonomes, aînés, etc.)

.

CHAPITRE V

CONCLUSION

À la lumière des résultats obtenus et suite aux discussions et analyses de ceux-ci, il est raisonnable de considérer l'activité de recherche et sa communication close. Il est donc temps de résumer les principales conclusions de celle-ci.

5.1 Conclusions

Les principales conclusions qui se dégagent des résultats est qu'il existe une possibilité de changement permettant de réduire l'écart entre les besoins des utilisateurs en matière de GIDIM qui ne sont pas exprimés dans le processus de conception et la réalité des principales plateformes mobiles. Cet écart commence d'ailleurs à être comblé, notamment par *Knox*, qui répond à nombre d'insatisfactions générales concernant la GIDIM classique. Or, cette voie se basse essentiellement sur les considérations d'autrui (principalement les employeurs) pour les UFs et laisse quand-même vacante la position de leadership à cet effet. Il y a des motifs pour lesquels cette place reste vide et c'est essentiellement parce que la satisfaction de ces besoins n'est pas simple, d'autant plus que ces besoins sont souvent contradictoires. Par conséquent, le fait d'offrir une pluralité d'options semble avoir été une des clés à la solution de ce problème.

Les modes d'opération recensés sont au nombre de treize (13). Ce nombre n'est pas définitif, pas plus que les modes eux-mêmes. Il existe d'autres manières de segmenter les types d'utilisation et celles-ci devraient être proposées, mises de l'avant, comparées et mises à l'épreuve de l'adoption par les UFs. Les plateformes actuelles ont été analysées, avec une emphase sur ce qui semble être l'état actuel le plus récent de la réflexion en matière d'intégration des besoins des UFs en matière de GIDIM, soit *Samsung Knox*.

Il est donc proposé de conclure que la présente recherche a atteint ses objectifs à l'intérieur de la portée qui était fixée.

5.2 Inscription dans la durée

Il est important de rappeler que la situation actuelle n'est pas sombre, elle est cependant grandement perfectible. Bien que les faits observés et la littérature consultée aient permis de déceler une multitude de moyens d'améliorer la situation ainsi que certains risques et appréhensions perçus, il n'y a pas matière à s'alarmer. Le processus d'amélioration semble correspondre à un cycle de vie lent et qui s'inscrit dans la durée. De par ce constat, une stratégie de conciliation et de consensus devrait guider le développement.

Les décisions d'aujourd'hui sont de nature à affecter la qualité de vie et le contexte politique des UFs dans l'avenir. La technologie accroît tellement la capacité applicative, la « faculté de faire », qu'elle est devenue un enjeu politique, tant à l'intérieur des sociétés qu'entre les nations. Ces nations qui s'organisaient traditionnellement en des hiérarchies, selon de fragiles équilibres de contrôles de ressources, ont ensuite formé des États, toujours sur une base de contrôle de ressources. Or, dans un contexte où ces ressources sont de moins en moins matérielles, les États eux-mêmes se trouvent fragilisés et certains acteurs privés prennent le dessus du pavé, toujours au travers des contrôles de ressources comparables à ceux de certains pays, voire de certaines fédérations. Dans le cas de Google, la diversité de ses recherches, notamment dans la sphère possiblement militaire, avec leur brève incursion dans l'aventure *Boston Dynamics*, laisse poindre la possibilité que certains de ces acteurs privés aient des visées de se substituer, éventuellement, dans un avenir lointain, aux États. Du côté d'*Apple*, ce sont la ferveur et la fierté d'appartenance, à la communauté de ses utilisateurs, qui semblent être sans commune mesure avec l'état actuel du patriotisme actuel dans un contexte mondialisé.

Ainsi, bien que certains éléments de la présente étude aient pu sembler voisins de l'approche des théories critiques, il faut garder à l'esprit que le but de d'exprimer les besoins des utilisateurs n'ayant longtemps eu aucune voix au chapitre est simplement de

préserver l'adhésion à des préceptes et une utilisation des technologies mobiles qui soit saine et qui favorise ce pour quoi les TIC sont conçues, à la base : tisser et renforcer des liens entre des êtres sociaux. Cela requiert une intégration de besoins parfois discordants, mais qui sont tous nécessaires pour l'atteinte de ce but de communication.

5.3 Intégration dans le processus de développement

Attendu la nature de cette technologie ainsi que l'évolution rapide et la concurrence, il serait souhaitable, pour les étapes ultérieures de développement de retenir une méthode agile ou probablement celle du prototype minimalement fonctionnel. Avec une diversité de prototypes et une instrumentation adéquate, ainsi qu'avec de la rétroaction de la part de la communauté ou de groupes spécifiquement suivis à des fins d'analyse, il serait envisageable d'avoir une expression des besoins des UFs qui soit assez proche de la réalité.

5.4 Remarques finales

Tout au long de ce processus de recherche, au fil des douze (12) ans (incluant une portion hors-académie de cinq (5) ans, ayant permis d'investir dans des projets aussi rétributeurs en termes financiers qu'en termes de connaissance sur le sujet de la GIDIM), qu'a durée cette recherche, il a été intéressant de voir naître et évoluer ce phénomène. Cette place d'observateur privilégié a cependant requis l'apport extraordinairement utile des nombreux conseillers dont le principal défi aura été de garder la concentration sur l'étude rigoureuse d'un phénomène riche sous le filtre de la recherche académique et l'auteur de la présente étude ne saurait assez les remercier pour cela.

APPENDICES

APPENDICE A

EXTRAITS CONTRACTUELS (APPLE)

(c) Dans la mesure où Apple a préinstallé des applis de marque Apple de l'App Store sur l'appareil iOS que vous achetez (« Applis préinstallées »), vous devez vous connecter à l'App Store et associer lesdites applis avec votre compte afin de les utiliser sur votre appareil iOS. Lorsque vous associez une appli préinstallée à votre compte de l'App Store, toutes les autres applis préinstallées de votre appareil iOS sont automatiquement associées à ce compte. En choisissant d'associer les applis préinstallées à votre compte de l'App Store, vous acceptez qu'Apple puisse transmettre, rassembler, conserver, traiter et utiliser l'identifiant Apple correspondant à votre compte de l'App Store et un identifiant matériel unique transmis par votre appareil iOS comme identifiants uniques de votre compte afin de vérifier l'éligibilité de votre requête et de fournir l'accès aux applis préinstallées via l'App Store.

Vous ne pouvez ni louer, ni louer en crédit bail, ni prêter, ni vendre, ni redistribuer, ni concéder de sous-licences du Logiciel iOS. Vous pouvez toutefois effectuer le transfert unique et permanent de tous vos droits sur le Logiciel iOS à une autre partie dans le cadre du transfert de propriété de votre appareil iOS, à condition : (a) que ce transfert comprenne votre appareil iOS et la totalité du Logiciel iOS, y compris l'intégralité de ses composants, données d'origine, documents imprimés ainsi que cette Licence; (b) que vous ne conserviez aucune copie du Logiciel iOS, complète ou partielle, y compris toute copie stockée sur ordinateur ou toute autre unité de stockage; et (c) que la partie bénéficiaire recevant le Logiciel iOS prenne connaissance et accepte les conditions générales de la présente Licence.

4. Accord relatif à l'utilisation des données. Lorsque vous utilisez votre appareil, votre numéro de téléphone et certains identifiants uniques à votre appareil iOS sont envoyés à Apple afin de permettre à d'autres personnes de vous joindre par votre numéro de téléphone lors de l'utilisation de diverses fonctionnalités de communication du Logiciel iOS, telles qu'iMessage et Facetime. Lorsque vous utilisez iMessage, Apple peut conserver vos messages sous forme encodée pendant une période limitée dans le but d'assurer leur livraison. Vous pouvez désactiver Facetime ou iMessage en vous rendant dans les réglages

FaceTime ou Messages de votre appareil iOS. Certaines fonctionnalités comme Diagnostic et Utilisation, Services de localisation, Siri, Dictée et Spotlight peuvent nécessiter des informations de la part de votre appareil iOS afin d'exécuter leurs fonctions respectives. Lorsque vous activez ou utilisez ces fonctionnalités, des détails seront fournis au sujet des informations envoyées à Apple et de la façon dont elles peuvent être utilisées. Vous pouvez en savoir plus en visitant http://www.apple.com/ca/fr/ privacy/. En tout temps, vos informations sont traitées conformément à l'Engagement de confidentialité d'Apple disponible à l'adresse : http://www.apple.com/legal/privacy/.

9. Certificats numériques. Le Logiciel iOS inclut des fonctionnalités permettant d'accepter des certificats numériques émis soit par Apple, soit par des tiers. VOUS ÊTES PAR CONSÉQUENT RESPONSABLE DÈS LORS QUE VOUS DÉCIDEZ DE FAIRE CONFIANCE À UN CERTIFICAT, QU'IL PROVIENNE D'APPLE OU D'UN TIERS. L'UTILISATION DE CERTIFICATS NUMÉRIQUES RESTE À VOS RISQUES ET PÉRILS. DANS TOUTE LA MESURE PERMISE PAR LA LOI EN APPLICATION, APPLE NE DONNE AUCUNE GARANTIE OU REPRÉSENTATION, EXPRESSE OU IMPLICITE, QUANT À LA QUALITÉ MARCHANDE OU L'ADÉQUATION À UN USAGE PARTICULIER, LA PRÉCISION, LA SÉCURITÉ OU LA NON-VIOLATION DES DROITS DE TIERS CONCERNANT LES CERTIFICATS NUMÉRIQUES.

12. Loi applicable et divisibilité du contrat. Cette licence est régie et interprétée en conformité avec la législation de l'État de Californie, mis à part les conflits en matière de principes légaux. Cette licence n'est pas régie par la convention des Nations Unies sur les contrats de vente internationale de biens, dont l'application est expressément exclue. Si vous êtes un client basé dans au Royaume-Uni, la présente Licence est régie par la législation de votre juridiction. Si pour une raison quelconque un tribunal ayant juridiction juge qu'une stipulation de la Licence est inapplicable, en totalité ou en partie, les autres stipulations de la Licence restent entièrement applicables.

Extraits de la politique de confidentialité d'Apple.

Lorsque vous êtes en communication avec Apple ou ses sociétés affiliées, vous pourriez devoir à n'importe quel moment fournir des renseignements personnels. Apple et ses sociétés affiliées peuvent se partager ces renseignements personnels et les utiliser conformément à la présente politique de confidentialité. Elles peuvent aussi les combiner avec d'autres renseignements afin d'offrir nos produits, services, contenus et publicités et de les améliorer. Vous n'êtes pas obligé de nous communiquer les renseignements personnels que nous vous demandons. Cependant, si vous choisissez de ne pas les communiquer, nous ne pourrons pas toujours vous fournir nos produits et services, ou même répondre à vos questions.

Lorsque vous créez un identifiant Apple, demandez un crédit commercial, achetez un produit, téléchargez une mise à jour logicielle, vous inscrivez à un cours donné dans un Apple Store, communiquez avec nous ou participez à un sondage en ligne, nous pouvons collecter divers renseignements, y compris vos nom, adresse postale, numéro de téléphone, adresse courriel et préférences de communication, ainsi que vos renseignements de cartes de crédit.

Lorsque vous partagez votre contenu avec vos amis et votre famille à l'aide de produits Apple, que vous envoyez des chèques-cadeaux et des produits ou que vous invitez des personnes à participer aux services ou aux forums Apple, Apple peut recueillir les renseignements que vous fournissez sur ces personnes, y compris leur nom, adresse postale, adresse courriel et numéro de téléphone. Apple utilisera ces renseignements afin de répondre à vos demandes, de vous offrir les produits ou les services applicables ou encore à des fins de lutte contre la fraude.

Dans certains pays, nous pouvons demander une pièce d'identité émise par le gouvernement dans certaines situations, notamment pour la création d'un compte de téléphonie mobile et l'activation de votre appareil, la détermination de l'admissibilité au crédit commercial, la gestion des réservations ou si la loi l'exige.

Extrait des clauses des services Internet d'Apple

« These terms and conditions create a contract between you and Apple (the "Agreement"). Please read the Agreement carefully. To confirm your understanding and acceptance of the Agreement, click "Agree."

A. INTRODUCTION TO OUR SERVICES

This Agreement governs your use of Apple's services ("Services"), through which you can buy, get, license, rent or subscribe to media, apps ("Apps"), and other in-app services ("Content"). Our Services are: iTunes Store, App Store, iBooks Store, Apple Music, and Apple News. Our Services are available for your use in your country of residence ("Home Country"). To use our Services, you need compatible hardware, software (latest version recommended and sometimes required) and Internet access (fees may apply). Our Services' performance may be affected by these factors. »

CONTRACT CHANGES

Apple reserves the right at any time to modify this Agreement and to add new or additional terms or conditions on your use of the Services. Such modifications and additional terms and conditions will be effective immediately and incorporated into this Agreement. Your continued use of the Services will be deemed acceptance thereof.

You agree that the Services, including but not limited to Content, graphics, user interface, audio clips, video clips, editorial content, and the scripts and software used to implement the Services, contain proprietary information and material that is owned by Apple and/or its licensors, and is protected by applicable intellectual property and other laws, including but not limited to copyright. You agree that you will not use such proprietary information or materials in any way whatsoever except for use of the Services for personal, noncommercial uses in compliance with this Agreement. No portion of the Services may be reproduced in any form or by any means, except as expressly permitted by this Agreement. You agree not to

modify, rent, loan, sell, or distribute the Services or Content in any manner, and you shall not exploit the Services in any manner not expressly authorized.

Extrait des conditions de iTunes

MODIFICATIONS À L'ENTENTE

Apple se réserve le droit, à tout moment, de modifier la présente Entente et d'imposer de nouvelles conditions générales concernant votre utilisation des Services. Ces modifications et conditions générales supplémentaires entreront en vigueur immédiatement et seront incorporées à la présente Entente. Votre utilisation continue des Services sera considérée comme l'expression de votre acceptation de l'ensemble de ces clauses supplémentaires.

Extrait de conditions de iCloud

Apple est le fournisseur du Service qui vous permet d'utiliser certains services Internet, y compris de stocker vos données personnelles (telles que les contacts, calendriers, photos, notes, rappels, documents, données d'application et messagerie iCloud) et les rendre accessibles sur vos appareils et ordinateurs compatibles, et certains services de géolocalisation, et ce conformément aux conditions générales du présent Contrat. iCloud s'active automatiquement lorsque vous utilisez des appareils sous iOS 9 ou ultérieur et que vous ouvrez une session par le biais de votre identifiant Apple pendant la configuration de l'appareil, à moins que vous ne mettiez à niveau l'appareil après avoir choisi de ne pas activer iCloud. Vous pouvez désactiver iCloud dans Réglages. Quand iCloud est activé, votre contenu est automatiquement envoyé à et stocké par Apple, afin que vous puissiez y accéder plus tard ou qu'il soit transmis via les réseaux sans fil (en mode push) vers vos autres appareils ou ordinateurs compatibles iCloud.

A. Âge Le Service n'est disponible que pour les personnes âgées de 13 ans ou plus (ou d'un âge minimum équivalent dans la juridiction applicable), à moins que votre identifiant Apple vous ait été fourni à la suite d'une demande effectuée par un établissement de formation agréé ou qu'il ait été établi par vos parents ou votre tuteur légal comme appartenant à la fonction de partage familial. Nous ne recueillons, n'utilisons ni ne divulguons des informations personnelles d'enfants de moins de 13 ans, ou de l'âge minimum équivalent dans la juridiction appropriée, sans l'accord vérifiable des parents. Les parents ou tuteurs légaux doivent également rappeler aux mineurs qu'il peut être dangereux de dialoguer avec des étrangers sur Internet et prendre les mesures appropriées pour protéger les enfants, y compris en surveillant leur utilisation du Service.

Pour utiliser le Service, rien ne doit vous empêcher de l'utiliser en vertu des lois des États-Unis ou d'autres juridictions applicables, y compris celles du pays dans lequel vous résidez ou à partir duquel vous utilisez le Service. En acceptant ce Contrat, vous déclarez avoir compris et accepté ce qui précède.

B. Appareils et Comptes L'utilisation du Service peut requérir des appareils compatibles, un accès à Internet et certains logiciels (des frais peuvent s'appliquer) ; peut nécessiter des mises à jour périodiques ; et peut être affectée par la performance de ces facteurs. Apple se réserve le droit de limiter le nombre de Comptes pouvant être créés à partir d'un appareil et le nombre d'appareils associés à un Compte. La dernière version du logiciel nécessaire peut être requise pour certaines transactions ou fonctionnalités. Vous acceptez qu'il soit de votre responsabilité de remplir ces conditions.

C. Restrictions d'utilisation Vous acceptez d'utiliser le Service uniquement pour les finalités autorisées par le présent Contrat et conformément aux lois et réglementations applicables, ou aux pratiques généralement acceptées dans la juridiction applicable.

E. Modification du Service Apple se réserve le droit de modifier à tout moment le présent Contrat et d'imposer des conditions nouvelles ou supplémentaires concernant l'utilisation du Service, dans la mesure où Apple vous donne un préavis de 30 jours d'un quelconque changement défavorable d'élément lié au Service ou condition d'utilisation applicable, à moins qu'il ne soit pas raisonnable en raison de circonstances découlant d'une action légale, réglementaire ou gouvernementale, pour répondre à des soucis de sécurité de l'utilisateur, de confidentialité de l'utilisateur ou d'intégrité technique, pour éviter les interruptions de service vis-à-vis des autres utilisateurs ou en raison d'une catastrophe naturelle ou d'autre nature, d'une guerre ou d'autre événement assimilable en dehors du contrôle raisonnable d'Apple. Eu égard aux services payants de stockage en ligne, Apple n'apportera aucun changement défavorable d'élément au Service avant la fin de votre terme payant en cours, à moins qu'un changement ne soit raisonnablement nécessaire pour satisfaire à une action légale, réglementaire ou gouvernementale ; pour répondre à des soucis de sécurité de l'utilisateur, de confidentialité de l'utilisateur ou d'intégrité technique ; pour éviter les interruptions de service vis-à-vis des autres utilisateurs ; ou pour éviter des problèmes découlant d'une catastrophe naturelle ou d'autre nature, d'une guerre ou d'autre événement assimilable en dehors du contrôle raisonnable d'Apple. Au cas où Apple ne procède pas à des changements défavorables d'élément du Service ou de conditions d'utilisation, vous disposez du droit de

résilier le présent Contrat et votre compte, auquel cas Apple vous proposera un remboursement au prorata de tout prépaiement de votre terme payant en cours. Apple ne saurait être responsable envers vous de toute modification du Service ou conditions d'utilisation, réalisée en conformité avec la présente Section I-E.

A. Utilisation des services de géolocalisation

Apple, ses partenaires et concédants peuvent fournir certaines fonctionnalités ou services (par exemple, Localiser mon iPhone, Localiser mes Amis) qui s'appuient sur des informations de localisation provenant des appareils qui utilisent le système GPS (lorsqu'il est disponible), ainsi que des points d'accès hot-spot Wi-Fi publics et les localisations de tours de téléphonie mobile. Pour fournir ces fonctionnalités ou services lorsqu'ils sont disponibles, Apple, ses partenaires et concédants doivent recueillir, utiliser, transmettre, traiter et conserver vos données de localisation, y compris, notamment, la localisation géographique de votre appareil et de l'information liée à votre compte iCloud (« Compte ») et tout autre appareil enregistré ci-dessous, et, notamment, votre identifiant Apple, nom et identifiant d'appareil, et type d'appareil.

A. Votre Compte

En tant qu'utilisateur inscrit au Service, vous devez créer un Compte. Ne communiquez pas les informations de votre Compte à quiconque. Vous êtes seul responsable du maintien de la confidentialité et de la sécurité de votre Compte et de toutes les activités liées à votre Compte ou par son biais, et vous acceptez de signaler immédiatement à Apple toute faille de sécurité de votre Compte. Vous reconnaissez et acceptez également que le Service est conçu et destiné à un usage personnel et de manière individuelle et que vous vous abstiendrez de partager les informations de votre Compte ou mot de passe avec toute autre personne. Sous réserve d'avoir fait preuve de compétence raisonnable et de diligence, Apple ne pourra être responsable des pertes résultant de l'utilisation non autorisée de votre Compte et du non-respect de ces règles.

Afin d'utiliser le Service, vous devez saisir votre identifiant Apple et votre mot de passe pour authentifier votre Compte. Vous acceptez de fournir des informations exactes et complètes lors de votre inscription, et lorsque vous utilisez, le Service (« Données d'inscription au Service »), et vous acceptez de mettre à jour vos Données d'inscription au Service pour assurer qu'elles sont exactes et complètes. Toute omission de fournir des Données d'inscription au Service exactes, actuelles et complètes peut entraîner l'interruption ou la résiliation de votre Compte. Vous acceptez qu'Apple stocke et utilise les Données d'inscription au Service que vous fournissez dans le but de traiter et facturer les frais de votre Compte.

C. Absence de transfert de droit

Aucune disposition du présent Contrat ne doit avoir pour effet de vous conférer tout intérêt, titre ou licence concernant un identifiant Apple, une adresse e-mail, un nom de domaine, un identifiant iChat ou une ressource similaire utilisée par vous en relation avec le Service.

D. Absence de transmission en cas de décès

Sauf obligation contraire imposée par la loi, vous acceptez que votre Compte est incessible et que tous les droits liés à votre identifiant Apple ou Contenu dans le cadre de votre Compte seront résiliés au moment de votre décès. Dès réception d'une copie d'un certificat de décès, votre Compte pourra être résilié et l'intégralité du Contenu de votre Compte pourra être supprimée. Pour plus d'assistance, veuillez contacter notre Assistance iCloud à l'adresse https://www.apple.com/support/iCloud/.

Vous acceptez de ne PAS utiliser le Service pour :

a. télécharger, publier, envoyer par courrier électronique, transmettre, conserver ou rendre disponible tout Contenu illégal, harcelant, menaçant, nuisible, délictueux, diffamatoire,

injurieux, abusif, violent, obscène, vulgaire, indiscret quant à la vie privée d'un tiers, haineux, injurieux à l'égard d'une race ou ethnie, ou choquant ;

b. poursuivre, harceler, menacer ou nuire à une autre personne ;

c. si vous êtes un adulte, demander des données personnelles ou autres à un mineur (toute personne âgée de moins de 18 ans ou ayant un âge qui la définit comme mineure selon les lois de son pays) que vous ne connaissez pas personnellement, y compris notamment, l'une des informations suivantes : le nom complet ou le nom de famille, l'adresse personnelle, le code postal, le numéro de téléphone, la photo ou le nom de l'école, de l'église, de l'équipe sportive ou des amis de ce mineur ;

d. prétendre être une personne que vous n'êtes pas ou représenter une entité à laquelle vous n'appartenez pas – vous ne pouvez imiter ou vous faire passer pour une autre personne (célébrités comprises), une autre entité, un autre utilisateur du service iCloud, un employé d'Apple, ou un chef de gouvernement ou une personnalité locale, ou présenter de manière inexacte votre affiliation auprès d'une personne ou entité (Apple se réserve le droit de rejeter ou bloquer tout identifiant Apple ou adresse e-mail pouvant être considéré comme l'imitation ou la représentation erronée de votre identité ou l'appropriation frauduleuse du nom et de l'identité d'une autre personne) ;

C. Suppression de Contenu

Vous reconnaissez qu'Apple ne puisse en aucun cas être tenue pour responsable du Contenu fourni par d'autres et n'a aucune obligation d'examiner au préalable ce Contenu. Cependant, Apple se réserve le droit de déterminer à tout moment si le Contenu est approprié et conforme au présent Contrat, et peut examiner au préalable, déplacer, refuser, modifier ou supprimer à tout moment du Contenu, sans préavis et à son entière discrétion, si ce Contenu s'avère contraire aux dispositions du présent Contrat ou est autrement contestable.

1. Licence concédée par vous À l'exception des informations pour lesquelles nous vous concédons une licence, Apple ne revendique aucun droit sur les informations ou le Contenu que vous publiez ou mettez à disposition grâce au Service. Cependant, en publiant ce Contenu sur des parties du Service accessibles au public ou à d'autres utilisateurs avec lesquels vous acceptez de partager ce Contenu, vous concédez à Apple une licence pour le monde entier, à titre gratuit, non exclusive, d'utilisation, de distribution, de reproduction, de modification, d'adaptation, de publication, de traduction, d'exécution et de diffusion publique du Contenu sur le Service uniquement aux fins pour lesquelles un tel Contenu a été publié ou mis à disposition, sans aucune compensation ou obligation envers vous. Vous acceptez que tout contenu que vous publiez soit sous votre seule responsabilité, que ce Contenu ne constitue pas une contrefaçon ou ne viole pas les droits de tiers ou ne viole pas les lois, ne constitue pas un acte illégal ou n'en encourage pas, ni ne soit jugé obscène ou choquant. En publiant ce Contenu dans des parties du Service accessibles au public ou à d'autres utilisateurs, vous déclarez être le propriétaire de cette information ou bénéficier de tous les droits, licences et autorisations nécessaires pour de telles publications.

A. Résiliation volontaire de votre part

Vous pouvez supprimer votre identifiant Apple ou arrêter d'utiliser le Service à tout moment. Si vous souhaitez arrêter d'utiliser iCloud sur votre appareil, vous pouvez désactiver iCloud sur un appareil en accédant aux Réglages de votre appareil, en tapant sur iCloud, puis sur « Se déconnecter ». Pour résilier votre Compte et supprimer votre identifiant Apple, contactez l'Assistance d'Apple à l'adresse http://apple.com/fr/support/appleid/contact. Si vous résiliez votre compte et supprimez votre identifiant Apple, vous n'aurez pas accès aux autres produits et services Apple par le biais de cet identifiant Apple. Il se peut que cette opération soit irréversible. Tous les frais payés avant votre résiliation ne sont pas remboursables (sauf autorisation expresse contraire au présent Contrat), y compris tous les frais payés d'avance pour l'année de facturation en cours. La résiliation de votre Compte ne vous dégage d'aucune obligation de payer d'éventuels frais accumulés.

B. Résiliation par Apple

Apple peut à tout moment, dans certains cas et sans préavis, résilier immédiatement ou suspendre tout ou partie de votre Compte ou de l'accès au Service. Les causes d'une telle résiliation peuvent inclure : (a) les violations du présent Contrat ou de toute autre politique ou directive mentionnée dans les présentes ou publiée sur le Service ; (b) la demande de votre part d'annuler ou de résilier votre Compte ; (c) la demande ou l'injonction d'autorités judiciaires ou administratives ; (d) lorsque le fait de vous fournir le Service est ou peut devenir illégal ; (e) des problèmes techniques ou de sécurité inattendus ; (f) votre participation à des activités frauduleuses ou illégales ; ou (g) l'omission de payer les frais que vous devez en relation avec le Service, hormis dans le cas d'une violation non substantielle, Apple ne sera autorisé à résilier le Contrat qu'après vous l'avoir communiqué avec un préavis de 30 jours et que si vous n'avez pas remédié à ladite violation dans le délai de 30 jours en question. Une telle résiliation ou suspension sera effectuée par Apple à son entière discrétion, et Apple ne pourra être tenue responsable envers vous ou un tiers des dommages pouvant résulter ou survenir suite à cette résiliation ou suspension de votre Compte ou de l'accès au Service. De plus, Apple peut résilier votre Compte sur préavis de 30 jours en vous adressant un e-mail à l'adresse associée à votre identifiant Apple si (a) votre compte est inactif depuis un (1) an ; ou (b) s'il existe une interruption généralisée affectant le Service ou toute partie de celui-ci. L'avis de cessation générale du service sera fourni comme énoncé par la présente, à moins qu'il ne soit pas raisonnable de procéder ainsi en raison de circonstances découlant d'une action légale, réglementaire ou gouvernementale, pour répondre à des soucis de sécurité de l'utilisateur, de confidentialité de l'utilisateur ou d'intégrité technique, pour éviter les interruptions de service vis-à-vis des autres utilisateurs ou en raison d'une catastrophe naturelle ou d'autre nature, d'une guerre ou d'autre événement assimilable en dehors du contrôle raisonnable d'Apple. En cas d'une telle résiliation, Apple vous proposera un remboursement au prorata de tout prépaiement de votre terme payant en cours. Apple ne saurait être responsable envers vous de toute modification du Service ou conditions d'utilisation, en conformité avec la présente Section VII-B.

C. Effets de la résiliation

Dès la résiliation de votre Compte, il se peut que vous perdiez tout accès au Service, en totalité ou en partie, y compris, mais sans s'y limiter, votre Compte, votre identifiant Apple, votre compte de messagerie et votre Contenu. De plus, après un certain laps de temps, Apple supprimera les informations et données stockées dans, ou en lien avec, vos comptes. Tout composant individuel du Service que vous pouvez avoir utilisé et qui fait l'objet de contrats de licence séparés sera également résilié, conformément à ces contrats de licence.

B. Loi en vigueur

Sauf disposition contraire dans la section suivante, le présent Contrat et la relation entre vous et Apple sont soumis aux lois de l'État de Californie, à l'exclusion de ses dispositions sur les conflits de lois. Vous et Apple acceptez de vous soumettre à la juridiction personnelle et exclusive des tribunaux du comté de Santa Clara, Californie, pour résoudre les litiges et réclamations relatifs au présent Contrat. Si (a) vous n'êtes pas un citoyen américain ; (b) vous ne résidez pas aux États-Unis ; (c) vous n'accédez pas au Service à partir des États-Unis et (d) vous êtes un citoyen de l'un des pays identifiés ci-dessous, vous reconnaissez par la présente que les litiges ou réclamations résultant du présent Contrat seront soumis à la loi applicable énoncée ci-dessous, à l'exclusion des dispositions sur les conflits de loi, et vous acceptez par la présente la compétence non-exclusive des tribunaux situés dans l'état, la province ou le pays identifié ci-dessous dont la loi est applicable :

Si vous êtes citoyen d'un des pays de l'Union européenne, de la Suisse, de la Norvège ou de l'Islande, les lois et la juridiction applicables seront celles de votre lieu habituel de résidence.

Toute application de la Convention des Nations Unies sur la vente internationale de marchandises au présent Contrat est expressément exclue.

C. Intégralité du Contrat

Ce Contrat constitue l'intégralité de l'accord entre vous et Apple, et régit votre utilisation du Service et remplace entièrement tout accord préalable entre vous et Apple concernant le Service. Vous pourrez également être soumis à des conditions générales complémentaires si vous utilisez des services associés, un contenu tiers ou des logiciels appartenant à des tiers. Si l'une des dispositions du présent Contrat est considérée nulle ou non opposable, cette disposition sera interprétée conformément au droit applicable afin de se rapprocher au mieux de l'intention initiale des parties, et les dispositions restantes resteront en vigueur. Le fait pour Apple de ne pas faire appliquer un droit ou une disposition découlant du présent Contrat ne constituera pas une renonciation de cette disposition. Vous acceptez, sauf disposition contraire expresse prévue dans le présent Contrat, qu'il n'y aura aucun tiers bénéficiaire du présent contrat.

APPENDICE B

EXTRAITS CONTRACTUELS (GOOGLE)

Bienvenue dans les règles de confidentialité de Google

Lorsque vous utilisez nos services, vous nous faites confiance pour le traitement de vos données. Les présentes règles de confidentialité visent à vous indiquer quelles informations nous collectons, pour quelle raison, et comment nous les utilisons. Ces règles sont importantes et nous espérons que vous prendrez le temps de les lire attentivement. Sachez que des fonctionnalités permettant de gérer vos données et de protéger votre confidentialité et votre sécurité sont disponibles dans la section Mon compte.
Règles de confidentialité
Masquer les exemples

Date de la dernière modification : 17 avril 2017 (voir les versions archivées)

Télécharger la version PDF

Vous pouvez avoir recours à nos services pour toutes sortes de raisons : pour rechercher et partager des informations, pour communiquer avec d'autres personnes ou pour créer des contenus. En nous transmettant des informations, par exemple en créant un compte Google, vous nous permettez d'améliorer nos services. Nous pouvons notamment afficher des annonces et des résultats de recherche plus pertinents et vous aider à échanger avec d'autres personnes ou à simplifier et accélérer le partage avec d'autres internautes. Nous souhaitons que vous, en tant qu'utilisateur de nos services, compreniez comment nous utilisons vos données et de quelles manières vous pouvez protéger votre vie privée.

Nos Règles de confidentialité expliquent :

les données que nous collectons et les raisons de cette collecte.

la façon dont nous utilisons ces données.

les fonctionnalités que nous vous proposons, y compris comment accéder à vos données et comment les mettre à jour.

Nous nous efforçons d'être le plus clair possible. Toutefois, si vous n'êtes pas familier, par exemple, des termes "cookies", "adresses IP", "balises pixel" ou "navigateurs", renseignez-vous préalablement sur ces termes clés. Chez Google, nous sommes soucieux de préserver la confidentialité de vos données privées. Ainsi, que vous soyez nouvel utilisateur ou un habitué de Google, prenez le temps de découvrir nos pratiques et, si vous avez des questions, n'hésitez pas à nous contacter.

Haut de la page

Données que nous collectons

Les informations que nous collectons servent à améliorer les services proposés à tous nos utilisateurs. Il peut s'agir d'informations de base, telles que la langue que vous utilisez, ou plus complexes, comme les annonces que vous trouvez les plus utiles, les personnes qui vous intéressent le plus sur le Web ou les vidéos YouTube qui sont susceptibles de vous plaire.

Nous collectons des données des manières suivantes :

Informations que vous nous communiquez : pour accéder à nos services, vous devez souvent créer un compte Google. Dans ce cas, vous fournissez des informations personnelles, telles que votre nom, votre adresse e-mail, votre numéro de téléphone ou votre carte de paiement, qui sont enregistrées avec votre compte. Pour pouvoir profiter de toutes les fonctionnalités de partage que nous proposons, vous pouvez également être amené à créer un profil Google public, qui peut comprendre votre nom et votre photo.

Informations que nous collectons lorsque vous utilisez nos services : nous collectons des informations relatives aux services que vous utilisez et à l'usage que vous en faites. Exemples : lorsque vous regardez une vidéo sur YouTube, lorsque vous vous rendez sur un site Web sur lequel nos services publicitaires sont utilisés ou lorsque vous consultez nos contenus et nos annonces, et que vous effectuez des actions sur celles-ci. Parmi ces informations, on peut citer :

Données relatives à l'appareil utilisé

Nous collectons des données relatives à l'appareil que vous utilisez, par exemple, le modèle, la version du système d'exploitation, les identifiants uniques de l'appareil et les informations relatives au réseau mobile, y compris votre numéro de téléphone. Nous sommes susceptibles d'associer les identifiants de votre appareil ou votre numéro de téléphone à votre compte Google.

Fichiers journaux

Lorsque vous utilisez nos services ou que vous affichez des contenus fournis par Google, nous collectons et stockons des informations dans les fichiers journaux de nos serveurs. Cela comprend :

la façon dont vous avez utilisé le service concerné, telles que vos requêtes de recherche.

des données relatives aux communications téléphoniques, comme votre numéro de téléphone, celui de l'appelant, les numéros de transfert, l'heure et la date des appels, leur durée, les données de routage des SMS et les types d'appels.

votre adresse IP.

des données relatives aux événements liés à l'appareil que vous utilisez, tels que plantages, activité du système, paramètres du matériel, type et langue de votre navigateur, date et heure de la requête et URL de provenance.

des cookies permettant d'identifier votre navigateur ou votre Compte Google de façon unique.

voici quelques extraits des conditions d'utilisation générales de Google

Les présentes Règles de confidentialité peuvent être amenées à changer. Toute diminution de vos droits dans le cadre des présentes Règles de confidentialité ne saurait être appliquée sans votre consentement exprès. Nous publierons toute modification des règles de confidentialité sur cette page et, dans le cas où il s'agirait de modifications significatives, nous publierons un avertissement mis en évidence (y compris, pour certains services, par le biais d'une notification par e-mail). Les versions antérieures des présentes Règles de confidentialité seront archivées et mises à la disposition des utilisateurs.

Votre compte Google

Vous pouvez avoir besoin d'un compte Google pour utiliser certains de nos Services. Votre compte Google peut être créé par vous-même ou vous être attribué par un administrateur (par exemple, votre employeur ou votre établissement d'enseignement). Si votre compte Google vous a été attribué par un administrateur, il se peut que des conditions d'utilisation différentes ou additionnelles s'appliquent et que votre administrateur puisse accéder à votre compte ou le désactiver.

Pour protéger votre compte Google, préservez la confidentialité de votre mot de passe. Vous êtes responsable de l'activité exercée dans votre compte Google ou par le biais de celui-ci. Veillez à ne pas réutiliser le même mot de passe que celui associé à votre compte Google, dans des applications tierces. Si vous découvrez que votre mot de passe ou votre compte Google a fait l'objet d'une utilisation non autorisée, suivez ces instructions.

Les Règles de confidentialité de Google expliquent comment nous traitons vos données à caractère personnel et protégeons votre vie privée lors de votre utilisation de nos Services. En utilisant nos Services, vous acceptez que Google puisse utiliser ces données conformément à ces Règles de confidentialité de Google.

Certains de nos Services vous permettent d'importer, de soumettre, de stocker, d'envoyer ou de recevoir des contenus. Vous conservez tous vos droits de propriété intellectuelle sur ces contenus. En somme, ce qui est à vous reste à vous.

Lorsque vous importez, soumettez, stockez, envoyez ou recevez des contenus à ou à travers de nos Services, vous accordez à Google (et à toute personne travaillant avec Google) une licence, dans le monde entier, d'utilisation, d'hébergement, de stockage, de reproduction, de modification, de création d'œuvres dérivées (des traductions, des adaptations ou d'autres modifications destinées à améliorer le fonctionnement de vos contenus par le biais de nos Services), de communication, de publication, de représentation publique, d'affichage public ou de distribution publique desdits contenus. Les droits que vous accordez dans le cadre de cette licence sont limités à l'exploitation, la promotion ou à l'amélioration de nos Services, ou au développement de nouveaux Services. Cette autorisation demeure pour toute la durée légale de protection de votre contenu, même si vous cessez d'utiliser nos Services (par exemple, pour une fiche d'entreprise que vous avez ajoutée à Google Maps). Certains Services vous proposent le moyen d'accéder aux contenus que vous avez soumis à ce Service et de les supprimer. Certains Services prévoient par ailleurs des conditions ou des paramètres restreignant la portée de notre droit d'utilisation des contenus que vous avez soumis aux Services en question. Assurez-vous que vous disposez de tous les droits vous permettant de nous accorder cette licence concernant les contenus que vous soumettez à nos Services.

Nos systèmes automatisés analysent vos contenus (y compris les e-mails) afin de vous proposer des fonctionnalités pertinentes sur les produits, telles que des résultats de recherche personnalisés, des publicités sur mesure et la détection des spams et des logiciels malveillants. Cette analyse a lieu lors de l'envoi, de la réception et du stockage des contenus.

Si vous disposez d'un compte Google, nous pouvons faire apparaître le nom et la photo de votre profil, et toute activité que vous exercez sur Google ou sur des applications tierces connectées à votre compte Google (telles que les +1 que vous attribuez, les avis que vous rédigez ou les commentaires que vous postez) au sein de nos Services, y compris dans le cadre de la diffusion d'annonces ou dans d'autres contextes commerciaux. Nous nous conformerons aux paramètres de partage ou de visibilité que vous définissez dans votre compte Google. Par exemple, vous pouvez définir vos paramètres pour que votre nom et votre photo n'apparaissent pas dans une annonce.

Vous trouverez des informations additionnelles sur la manière dont Google utilise et stocke les contenus dans les Règles de confidentialité ou éventuellement dans les conditions d'utilisation additionnelles associées à des Services particuliers. Lorsque vous nous soumettez des réactions ou des suggestions relatives à nos Services, nous sommes en droit de les utiliser sans solliciter votre autorisation.

Google n'a de cesse de modifier et d'améliorer ses Services. Nous sommes donc susceptibles d'ajouter ou de supprimer des fonctionnalités ou des fonctions, et il peut également arriver que nous suspendions ou interrompions complètement un Service.

Vous pouvez cesser d'utiliser nos Services à tout moment. Nous espérons cependant que vous continuerez de les utiliser. Google est en droit de cesser de vous fournir tout ou partie des Services, ou d'ajouter ou de créer de nouvelles limites à l'utilisation des Services et ce, à tout moment.

Pour nous, vous restez propriétaire des données que vous nous confiez et nous pensons qu'il est important que vous puissiez y accéder. Si nous devons interrompre un Service, dans la mesure du possible, nous vous en avertissons dans un délai raisonnable et vous donnons la possibilité de récupérer des informations de ce Service.

DANS LES LIMITES PERMISES PAR LA LOI, GOOGLE, SES FOURNISSEURS ET DISTRIBUTEURS, DÉCLINENT TOUTE RESPONSABILITÉ POUR LES PERTES DE BÉNÉFICES, DE REVENUS OU DE DONNÉES, OU LES DOMMAGES ET INTÉRÊTS INDIRECTS, SPÉCIAUX, CONSÉCUTIFS, EXEMPLAIRES OU PUNITIFS.

DANS LES LIMITES PERMISES PAR LA LOI, LA RESPONSABILITÉ TOTALE DE GOOGLE, DE SES FOURNISSEURS ET DISTRIBUTEURS, POUR TOUTE RÉCLAMATION DANS LE CADRE DES PRÉSENTES CONDITIONS D'UTILISATION, Y COMPRIS POUR TOUTE GARANTIE IMPLICITE, EST LIMITÉE AU MONTANT QUE VOUS NOUS AVEZ PAYÉ POUR UTILISER LES SERVICES (OU, SI TEL EST NOTRE CHOIX, POUR QUE NOUS VOUS FOURNISSIONS À NOUVEAU CES SERVICES).

EN AUCUN CAS, GOOGLE, SES FOURNISSEURS ET DISTRIBUTEURS NE SERONT TENUS RESPONSABLES POUR TOUTE PERTE OU DOMMAGE QUI N'AURAIT PAS ÉTÉ RAISONNABLEMENT PRÉVISIBLE.

Nous sommes susceptibles de modifier ces Conditions d'Utilisation ou toute autre condition d'utilisation complémentaire s'appliquant à un Service, par exemple, pour refléter des modifications de la loi ou de nos Services. Nous vous recommandons de consulter régulièrement les Conditions d'Utilisation. Les modifications apportées à ces Conditions d'Utilisation seront signalées sur cette page. Nous publierons un avis de modification des conditions d'utilisation additionnelles dans le Service concerné. Les modifications ne s'appliqueront pas de façon rétroactive et entreront en vigueur au moins quatorze (14) jours après leur publication. Toutefois, les modifications spécifiques à une nouvelle fonctionnalité d'un Service ou les modifications apportées pour des raisons juridiques s'appliqueront immédiatement. Si vous n'acceptez pas les modifications apportées aux Conditions d'Utilisation d'un Service donné, vous devez cesser toute utilisation de ce Service.

En cas de conflit entre ces Conditions d'Utilisation et des conditions d'utilisation additionnelles, ce sont ces dernières qui prévalent.

Ces Conditions d'Utilisation régissent votre relation avec Google. Elles ne créent pas de droit pour des tiers bénéficiaires.

Si vous ne respectez pas ces Conditions d'Utilisation et que nous ne prenons pas immédiatement de mesure à ce sujet, cela ne signifie pas que nous renonçons à nos droits (par exemple, à prendre une mesure ultérieurement).

S'il s'avère qu'une condition particulière n'est pas applicable, cela sera sans incidence sur les autres conditions de ces Conditions d'Utilisation.

Les éventuels litiges liés aux présentes Conditions d'Utilisation ou aux Services seront régis par les lois de l'État de Californie, États-Unis, à l'exclusion des règles de conflit de lois de cet État. Toute réclamation liée aux présentes Conditions d'Utilisation ou aux Services relèvera exclusivement de la juridiction des tribunaux fédéraux ou des tribunaux d'État du comté de Santa Clara, Californie, États-Unis. Google et vous-même acceptez par les présentes de vous soumettre à la compétence de ces tribunaux.

Pour toute information sur la procédure à suivre pour contacter Google, veuillez consulter la page de prise de contact.

NOTES DE RÉFÉRENCE

[1] Google says there are now 1.4 billion active Android devices worldwide - Android Central
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/18fa

[2] Le chef du SPVM admet avoir avalisé la surveillance de Patrick Lagacé - Louise Leduc - Actualités judiciaires
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/cmcc

[3] Tollé après la perquisition de la SQ au Journal de Montréal - ICI.Radio-Canada.ca
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/50aw

[4] Security Communication in Democracies
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/7v5r

[5] Commission d'enquête sur la protection de la confidentialité des sources journalistiques
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/x5pb

[6] NSA speaks out on Snowden, spying - CBS News
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/g4nk

[7] Rapport sur l'existence d'un système d'interception mondial des communications privées et économiques (système d'interception ECHELON) (2001/2098(INI))
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/l8fs

[8] Critical Factor sin Software Adoption. Dan Port, Ann Takenaka et David Klappholz. Stevens Institute of Technology
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/oe1z

[9] How to submit Feature Request - Forum d'assistance Thunderbird - Assistance de Mozilla
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/j1kf

[10] Fintech – The digital (r)evolution in the financial sector
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/pnpe

[11] Arner, D.; Barberis, J.; Buckley, R. (2016). The Evolution of FinTech: New Post-Crisis Paradigm. Georgetown Journal of International Law 47(4), 1271-1320.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/t451

[12] Bruce Bimber (2000) The Study of Information Technology and CivicEngagement, Political Communication, 17:4, 329-333, DOI: 10.1080/10584600050178924
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/fjr7

[13] Cyberdemocracy: Technology, cities and civic networks
C Bryan, D Tambini, R Tsagarousianou - 2002 - books.google.com
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/sh8e

[14] La « civic tech » veut favoriser la participation des citoyens
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/9bwa

[15] Southwell, K., James, K., Clarke, B.A., Andrews, B., Ashworth, C., Norris, M., and Patel, V. (Requirements Specification authoring team). Requirements Definition and Design.
The STARTS Guide, Second Edition, Volume I. National Computing Centre, 177-313, Chapter 5, 1987
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/1m98

[16] Competing Responsibilities
The Ethics and Politics of Contemporary Life
SUSANNA TRNKA and CATHERINE TRUNDLE, editors
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/rc0i

[17] Defossez, H. An Analysis about social tolerance.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/u72t

[18] Technical and Social History of Software Engineering
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/3455

[19] Designing for Social Impact. Gretchen Anderson
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/r23u

[20] Ahmadi, Navid et al. (2008). A Survey of Social Software Engineering. Proceedings of the 23rd IEEE/ACM International Conference on Automated Software Engineering. L'Aquila, Italie : IEEE Press.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/zefy

[21] NDT-Suite: A Methodological Tool Solution in the Model-Driven Engineering Paradigm written by Julián Alberto García-García, María José Escalona, Francisco José Domínguez-Mayo, Alberto Salido, published by Journal of Software Engineering and Applications, Vol.7 No.4, 2014
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/t9hm

[22] J. A. García-García, M. J. Escalona, E. Ravel, G. Rossi, and M. Urbieta. 2012. NDT-merge: a future tool for conciliating software requirements in MDE environments. In Proceedings of the 14th International Conference on Information Integration and Web-based Applications & Services (IIWAS '12). ACM, New York, NY, USA, 177-186. DOI=http://dx.doi.org/10.1145/2428736.2428765
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/iy4i

[23] Mark Blackburn and Robert Busser and Aaron Nauman. Why model-based test automation is different and what you should know to get started. 2004
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/pjmk

[24] Mark R. Blackburn and Robert Busser and Aaron Nauman. Removing Requirement Defects and Automating Test
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/7otf

[25] Mahamadou Touré. Introduction à l'épidémiologie MSO2000D, manuel de cours.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/kpq5

[26] Commission Charbonneau
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/b509

[27] Commission Bouchard Taylor
récupéré le 2013-07-01, depuis : http://uu1.ca/cite/xttc/1m37

[28] Requirements Engineering Fundamentals, 2nd Edition: A Study Guide for the Certified Professional for Requirements Engineering Exam – Foundation Level – IREB compliant
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/8a7m

[29] Lehtola, L. and Kauppinen, M. (2006), Suitability of requirements prioritization methods for market-driven software product development. Softw. Process: Improve. Pract., 11: 7–19.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/50ue

[30] Linking business and requirements engineering: is solution planning a missing activity in software product companies?
L. Lehtola, M. Kauppinen and S. Kujala, "Requirements Prioritization Challenges in Practice," Springer-Verlag, Berlin Heidelberg, 2004, pp. 497-508.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/8t6d

[31] M. Komssi, M. Kauppinen, H. Töhönen, L. Lehtola and A. M. Davis, "Integrating analysis of customers' processes into roadmapping: The value-creation perspective," 2011 IEEE 19th International Requirements Engineering Conference, Trento, 2011, pp. 57-66.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/awtw

[32] CITIZEN ENGAGEMENT AND MEDIA CAMPAIGN ON THE NEXT GENERATION INTERNET. Analysis and results of the launch of REIsearch 2.0. Atomium European Institute for science media and democracy
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/w2sd

[33] The Best Mobile Device Management (MDM) Solutions of 2017
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/nkpe

[34] Cisco Meraki Mobile device management
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/rzaj

[35] Application and Mobile Device Management (MDM) Microsoft
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/9chh

[36] Three reasons to choose Bell mobile device management
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/83pv

[37] The Forrester Wave™: Enterprise Mobile Management, Q4 2015; The 11 Providers That Matter Most And How They Stack Up.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/s864

[38] Enterprise Mobile Device Management Software MDM Cloud
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/uypd

[39] ManageEngine Mobile Device Management Admin Guide
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/4f89

[40] Mobile Device Management Symantec
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/6tqu

[41] Virtual instance architecture for mobile device management systems
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/qqut

[42] System And Method For Mobile Device Application Management
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/dhwf

[43] L. Liu, R. Moulic and D. Shea, "Cloud Service Portal for Mobile Device Management," 2010 IEEE 7th International Conference on E-Business Engineering, Shanghai, 2010, pp. 474-478.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/um0y

[44] Rhee K, Jeon W, Won D (2012) Security requirements of a mobile device management system. Int J Secur Appl 6(2):353---358
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/1g44

[45] Murugiah Souppaya et Karen Scarfone. 2013. NIST Special Publication 800-124, Revision 1. Guidelines for Managing the Security of Mobile Devices in the Enterprise.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/4g8o

[46] Rhee K., Eun SK., Joo MR., Jeong J., Won D. (2013) High-Level Design for a Secure Mobile Device Management System. In: Marinos L., Askoxylakis I. (eds) Human Aspects of Information Security, Privacy, and Trust. HAS 2013. Lecture Notes in Computer Science, vol 8030. Springer, Berlin, Heidelberg
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/exl7

[47] Pascaline — Wikipédia
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/gsa3

[48] History of Mechanical Calculators - Part I
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/nf2r

[49] How open sourcing Android made it a mobile market leader - Opensource.com
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/5lhe

[50] Vedran Dunjko, Jacob M. Taylor, and Hans J. Briegel. "Quantum-Enhanced Machined Learning." Physical Review Letters. DOI: 10.1103/PhysRevLett.117.130501
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/pq4l

[51] Google Play catching up with iOS App Store in volume, trails in revenue
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/be4t

[52] Google Play Catching Up to Apple's Apptore
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/6a8d

[53] It's 10 years since Google bought Android here are the highlights from Cupcake to Lollipop - AndroidPIT
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/jvyb

[54] Google buys Android - CNET
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/tpir

[55] Historique d'Android
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/txy7

[56] The history of Android
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/d8dk

[57] Android's early days - Android Central
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/b8eq

[58] The (updated) history of Android - Ars Technica
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/tkt6

[59] A History of Pre-Cupcake Android Codenames
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/4m78

[60] Kernel et Android Qu'est-ce que c'est et pourquoi le modifier - FrAndroid
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/d9yc

[61] Google Open Source – opensource.google.com
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/gpo8

[62] Google's fair use victory is good for open source - Ars Technica
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/19qy

[63] Google beats Oracle—Android makes "fair use" of Java APIs - Ars Technica
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/7h92

[64] ORACLE AMERICA, INC. v. GOOGLE INC.
Judge William H. Alsup. 10-CV-3561
Appeals from the United States District Court for the Northern District of California
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/h5lf

[65] La position de Google sur les brevets et l'open source (+ avis de Gibus) – Framablog
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/89ag

[66] Google's internal systems
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/4j3e

[67] Nicolae Sfetcu. Google Products, Services and Tools.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/wbcs

[68] James A. Whittaker,Jason Arbon,Jeff Carollo. How Google Tests Software
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/5yx9

[69] Google Search Appliance 7.6 - Google Enterprise Search
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/uqa6

[70] The Android Income Statement - Asymco
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/dpvp

[71] Android economics: An introduction
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/czri

[72] Lenovo Isn't Buying Motorola's Phones. It's Buying the Brand - Bloomberg
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/gm9k

[73] Apple's Partner Paradox
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/hgpg

[74] How Steve Jobs Played Hardball In iPhone Birth - WSJ
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/64rt

[75] Welcome to Planet Apple - Bloomberg
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/tn85

[76] Piper Jaffray: AT&T paying Apple $18 per iPhone, per month
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/kpx4

[77] Informez-vous de vos droits : ce que le Code du CRTC sur les services sans fil signifie pour vous
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/y7k1

[78] As Phone Subsidies Fade Apple Could Be Hurt - WSJ
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/l8yv

[79] Apple's iPhone Carrier Subsidies - Business Insider
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/gq2f

[80] Google's Open Source Android OS Will Free the Wireless Web - WIRED
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/jvjc

[81] Authors Guild v. Google Inc, 2nd U.S. Circuit Court of Appeals, No. 13-482
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/yuqy

[82] Actualités IT, logiciels et des acteurs d'internet - ZDNet.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/q0j8

[83] 3 Ways Google's In-App Search Will Influence Android App Development
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/wrb4

[84] Google launches new certification program for software development agencies
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/g5kf

[85] Joshua J. Drake wt al. Android Hacker's Handbook
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/durj

[86] Customer Letter - Apple
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/9g7q

[87] Chapter 1 Software Requirements - SWEBOK
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/y8mv

[88] Guide to the Software Engineering Body of Knowledge Version 3.0 (SWEBOK®). A Project of the IEEE Computer Society
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/cc60

[89] Leave my iPhone alone why our smartphones are extensions of ourselves - Technology - The Guardian
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/g9bq

[90] Wang, C., Lee, M., & Hua, Z. (2014). Understanding and Predicting Compulsive Smartphone Use: An Extension of Reinforcement Sensitivity Approach.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/el1d

[91] Clayton, R. B., Leshner, G. and Almond, A. (2015), The Extended iSelf: The Impact of iPhone Separation on Cognition, Emotion, and Physiology. J Comput-Mediat Comm, 20: 119–135. doi:10.1111/jcc4.12109
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/t8bp

[92] Clayton, R. B., Leshner, G. and Almond, A. (2015), The Extended iSelf: The Impact of iPhone Separation on Cognition, Emotion, and Physiology. J Comput-Mediat Comm, 20: 119–135. doi:10.1111/jcc4.12109
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/6zer

[93] version nc50 du présent mémoire
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/yqwi

[94] version j3tm du présent mémoire
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/hexe

[95] version 0mc0 du présent mémoire
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/tfle

[96] version 5q12 du présent mémoire
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/rc2z

[97] version sqea du présent mémoire
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/k9ai

[98] version fso2 du présent mémoire
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/qc5d

[99] version h013 du présent mémoire
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/6tg6

[100] Sécurité d'entreprise mobile - Samsung Knox
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/bjhx

[101] Freedom Of Contract Legal Definition - Merriam-Webster Law Dictionary
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/t6og

[102] Bruce A. Ackerman. Before the Next Attack: Preserving Civil Liberties in an Age of Terrorism
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/z1t8

[103] Ball, Kirstie and Webster, Frank eds. (2003). The Intensification of surveillance: crime, terrorism and warfare in the information era. London, UK: Pluto Press.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/9f0k

[104] Allmer, T. (2012). Critical internet surveillance studies and economic surveillance. Internet and Surveillance: the challenges of Web 2.0 and social media, 16(124), 683-683.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/qa1e

[105] EFF Action Center
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/7bq8

[106] LOI CONSTITUTIONNELLE DE 1982(80), PARTIE I, CHARTE CANADIENNE DES DROITS ET LIBERTÉS
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/tue0

[107] ZATAZ Les alternatives au système d'anonymisation TOR - ZATAZ
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/3v3h

[108] Surveillance Ethics - Internet Encyclopedia of Philosophy
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/maff

[109] With authoritarianism and state surveillance on the rise, how can civil society be protected from digital threats?
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/388o

[110] Décision de télécom CRTC 2016-479
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/6yjn

[111] Can Gambling Hurt Your Credit Score - Loans Canada
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/fb0f

[112] Credit Score Breakdown
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/fmnh

[113] Why Canadian sports gamblers bet billions offshore - CBC Sports - Sporting news, opinion, scores, standings, schedules
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/r6qv

[114] Online sports gambling thrives in Canada's legal 'grey zone' - CBC Sports - Sporting news, opinion, scores, standings, schedules
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/ddor

[115] How to get your bank statements mortgage-approval ready - Your Money
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/xacp

[116] What you buy, where you shop may affect your credit
New credit card law requires probe of issuers' use of purchasing data
By Connie Prater | Updated: October 14, 2009
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/430u

[117] Accueil - Le jeu doit rester un jeu - Loto-Québec
Mise Sur Toi
Association ou organisation
Adresse : 500 Rue Sherbrooke Ouest, Montréal, QC H3A 3C6
Téléphone : (514) 982-5524
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/68n8

[118] Ronald M. Pavalko. PROBLEM GAMBLING AND ITS TREATMENT: An Introduction
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/ssif

[119] Identity (Stanford Encyclopedia of Philosophy).
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/u8ct

[120] Encyclopédie Larousse en ligne - identité bas latin identitas -atis du latin classique idem le même.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/6otk

[121] Hube, J. P. (2007). Neyman-pearson biometric score fusion as an extension of the sum rule. Biometric Technology for Human Identification IV. Proceedings of the SPIE, 6539, 65390M.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/apds

[122] Anja Lehmann et al. Privacy and Identity Management. Facing up to Next Steps
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/hete

[123] Posted by: Margaret Rouse. What is identity management (ID management) - Definition from WhatIs.com
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/ujv7

[124] Michele Chubirka. A broader definition of identity governance
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/hn64

[125] Identity management - Wikipedia
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/j846

[126] Identity Management Basics
Derek Browne, CISSP, ISSAP
The OWASP Foundation
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/4hju

[127] BUYER'S GUIDE. Identity Management and Governance
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/n3mn

[128] Functional requirements for privacy enhancing systems
Fred Carter
Senior Policy & Technology Advisor
Office of the Information & Privacy Commissioner / Ontario, Canada
OECD Workshop on Digital Identity Management
Trondheim, Norway
09 May 2007
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/5der

[129] Archived NIST Technical Series Publication
NIST Special Publication 800-63 Version 1.0.2
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/cif9

[130] NIST Special Publication (SP) 800-63-2
Electronic Authentication Guideline
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/5zwr

[131] NIST Special Publication 800-63-3
Digital Identity Guidelines
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/nt48

[132] NIST Special Publication 800-63A
Digital Identity Guidelines. Enrollment and Identity Proofing
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/7aiv

[133] NIST Special Publication 800-63B
Digital Identity Guidelines
Authentication and Lifecycle Management
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/889q

[134] NIST Special Publication 800-63C
Digital Identity Guidelines
Federation and Assertions
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/5jy3

[135] ISO/IEC 24760-1 A framework for identity management—Part 1: Terminology and concepts
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/f05u

[136] ISO/IEC 24760-2 A Framework for Identity Management—Part 2: Reference architecture and requirements
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/6tnq

[137] ISO/IEC DIS 24760-3 A Framework for Identity Management—Part 3: Practice
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/bmvy

[138] ISO/IEC 29115 Entity Authentication Assurance
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/3rqe

[139] ISO/IEC 29146 A framework for access management
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/y73j

[140] ISO/IEC CD 29003 Identity Proofing and Verification
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/042a

[141] ISO/IEC 29100 Privacy framework
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/eyq3

[142] ISO/IEC 29101 Privacy Architecture
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/roc8

[143] ISO/IEC 29134 Privacy Impact Assessment Methodology
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/p0vp

[144] ElSalamouny, E., & Gambs, S. (2016). Differential privacy models for location-based services. Transactions on Data Privacy, 9(1), 15-48.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/zmgz

[145] Shokri, R., Theodorakopoulos, G., Le Boudec, J. Y., & Hubaux, J. P. (2011, May). Quantifying location privacy. In Security and privacy (sp), 2011 ieee symposium on (pp. 247-262). IEEE.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/6be0

[146] S. Gambs, M. O. Killijian and M. N. d. P. Cortez, "GEPETO: A GEoPrivacy-Enhancing TOolkit," 2010 IEEE 24th International Conference on Advanced Information Networking and
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/rfsd

[147] Sébastien Gambs, Marc-Olivier Killijian, and Miguel Núñez del Prado Cortez. 2010. Show me how you move and I will tell you who you are. In Proceedings of the 3rd ACM SIGSPATIAL International Workshop on Security and Privacy in GIS and LBS (SPRINGL '10). ACM, New York, NY, USA, 34-41. DOI=http://dx.doi.org/10.1145/1868470.1868479
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/2qea

[148] Gambs, S., Killijian, M. O., & del Prado Cortez, M. N. (2014). De-anonymization attack on geolocated data. Journal of Computer and System Sciences, 80(8), 1597-1614.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/6x1r

[149] Sébastien Gambs, Marc-Olivier Killijian, and Miguel Núñez del Prado Cortez. 2012. Next place prediction using mobility Markov chains. In Proceedings of the First Workshop on Measurement, Privacy, and Mobility (MPM '12). ACM, New York, NY, USA, Article 3, 6 pages.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/9zpi

[150] Bengio, S., Brassard, G., Desmedt, Y. G., Goutier, C., & Quisquater, J. J. (1991). Secure implementation of identification systems. Journal of Cryptology, 4(3), 175-183.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/hkey

[151] L. C. Guillou and J. J. Quisquater. 1990. A "paradoxical" identity-based signature scheme resulting from zero-knowledge. In Proceedings on Advances in cryptology (CRYPTO '88), Shafi Goldwasser (Ed.). Springer-Verlag New York, Inc., New York, NY, USA, 216-231.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/vkul

[152] Günther C.G. (1990) An Identity-Based Key-Exchange Protocol. In: Quisquater JJ., Vandewalle J. (eds) Advances in Cryptology — EUROCRYPT '89. EUROCRYPT 1989. Lecture Notes in Computer
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/1ypa

[153] Paul-Choudhury, S. (2011). Digital legacy: Respecting the digital dead. New Scientist Online.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/g0ex

[154] M. M. R. Chowdhury and J. Noll, "Distributed Identity for Secure Service Interaction," Wireless and Mobile Communications, 2007. ICWMC '07. Third International Conference on, Guadeloupe, 2007, pp. 56-56.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/v0rm

[155] N. Elahi, M. M. R. Chowdhury and J. Noll, "Semantic Access Control in Web Based Communities," 2008 The Third International Multi-Conference on Computing in the Global Information
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/pq4e

[156] J. Noll, S. Alam and M. M. R. Chowdhury, "Integrating Mobile Devices into Semantic Services Environments," 2008 The Fourth International Conference on Wireless and Mobile Communications, Athens, 2008, pp. 137-143.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/s15i

[157] Z. Iqbal, J. Noll, S. Alam and M. M. R. Chowdhury, "Toward User-Centric Privacy-Aware User Profile Ontology for Future Services," 2010 Third International Conference on Communication Theory, Reliability, and Quality of Service, Athens, TBD, Greece, 2010, pp. 249-254.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/1mfa

[158] Peterson, Z. N., Gondree, M., & Beverly, R. (2011). A position paper on data sovereignty: The importance of geolocating data in the cloud.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/48sv

[159] Irion, K. (2012). Government cloud computing and national data sovereignty. Policy & Internet, 4(3-4), 40-71.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/qphm

[160] Y. Nugraha, Kautsarina and A. S. Sastrosubroto, "Towards data sovereignty in cyberspace," 2015 3rd International Conference on Information and Communication Technology (ICoICT), Nusa Dua, 2015, pp. 465-471.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/rh5z

[161] Irion, Kristina (2011) : Government cloud computing and the policies of data sovereignty, 22nd European Regional Conference of the International Telecommunications Society (ITS2011), Budapest, 18 - 21 September, 2011: Innovative ICT Applications - Emerging Regulatory, Economic and Policy Issues
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/f19g

[162] Mosch, M. (2011). User-controlled data sovereignty in the Cloud. University Halle-Wittenberg Institute of Computer Science, 25.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/rsno

[163] Groß S., Schill A. (2012) Towards User Centric Data Governance and Control in the Cloud. In: Camenisch J., Kesdogan D. (eds) Open Problems in Network Security. Lecture Notes in Computer Science, vol 7039. Springer, Berlin, Heidelberg
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/o7jo

[164] Polatin-Reuben, D., & Wright, J. (2014). An Internet with BRICS Characteristics: Data Sovereignty and the Balkanisation of the Internet.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/q8e2

[165] Sargsyan, T. (2016). Data Localization and the Role of Infrastructure for Surveillance, Privacy, and Security. International Journal Of Communication, 10, 17.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/ebxs

[166] Shelton, D. (2006). Normative hierarchy in international law. American Journal of International Law, 100(2), 291-323.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/b5fa

[167] Eisenberg, R. (1989). Patents and the Progress of Science: Exclusive Rights and Experimental Use. The University of Chicago Law Review, 56(3), 1017-1086. doi:10.2307/1599761
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/h319

[168] Orlikowski, W. (1992). The Duality of Technology: Rethinking the Concept of Technology in Organizations. Organization Science, 3(3), 398-427.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/ubr3

[169] Venkatesh, V., Thong, J. Y., & Xu, X. (2012). Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/ecf1

[170] A Simple Authentication and Security Layer (SASL) and Generic Security Service Application Program Interface (GSS-API) Mechanism for OpenID
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/8xkc

[171] OpenID Authentication 2.0 - Final
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/ig43

[172] The OAuth 1.0 Protocol
IETF RFC 5849
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/eycm

[173] The OAuth 2.0 Authorization Framework
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/9e8z

[174] National Identity Management Commission Act
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/42vy

[175] Ley Orgánica 15_1999, de 13 de diciembre, de Protección de Datos de Carácter Personal
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/yzci

[176] Portal del DNI Electronico, Cuerpo Nacional de Policía
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/7yv3

[177] EU – eIDAS Regulation. Digital Single Market. Trust Services and eIdentification. Commission européenne.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/l89x

[178] eIDAS Regulation (Regulation (EU) N°910/2014)
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/1mak

[179] John Gregory . International Identity Management
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/9uot

[180] Colloque de la CNUDCI sur la gestion de l'identité et les services de confiance
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/i1fj

[181] Identity Management Legal Task Force. International Identity Management. Open Identity Exchange. Law and Policy Meeting. January 14, 2016
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/yz5z

[182] Loi concernant le cadre juridique des technologies de l'information
L.R.Q. (chapitre C-1.1)
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/bdrb

[183] Loi sur la protection des renseignements personnels
(L.R.C. (1985), ch. P-21)
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/m9bc

[184] Code civil du Québec
chapitre CCQ-1991
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/n1bo

[185] Loi sur la protection des renseignements personnels dans le secteur privé
chapitre P-39.1
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/29vz

[186] Google Inc. c. Equustek Solutions Inc.,
2017 CSC 34 (CanLII)
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/2bdz

[187] Chaire L.R. Wilson - Droit des technologies de l'information et du commerce électronique
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/1qvh

[188] Legal - Sales and Support - Apple.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/6ejx

[189] MFi Program - Apple Developer.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/0v7h

[190] Confidentialité - Apple (CA).
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/mgs6

[191] Legal - iCloud - Apple.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/10wi

[192] Legal - iCloud - Apple.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/q3y2

[193] MPEG LA - The Standard for Standards.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/008q

[194] Conditions d'utilisation de Google – Politique de confidentialité et conditions d'utilisation – Google.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/b9qu

[195] Politique de confidentialité – Politique de confidentialité et conditions d'utilisation – Google.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/841t

[196] Confidentialité - Notre approche - Apple (CA).
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/bolf

[197] Confidentialité - Gestion des paramètres - Apple (CA).
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/3vvc

[198] Confidentialité - Demandes du gouvernement - Apple (CA).
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/mpou

[199] Confidentialité - Redirect - Apple (CA).
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/gl52

[200] Apple (CA) - Informations juridiques - Conditions générales de service.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/jiux

[201] Chase, S. (1954). Power of words.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/71xb

[202] 159191 Canada inc. (Discount Location d'autos et camions) c. Waddell, 2013 QCCQ 3560
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/ylv3

[203] 159191 Canada inc. (Discount Location d'autos et camions) c. Waddell, 2013 QCCQ 3560 - LPC.quebec
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/pzva

[204] Dell Computer Corp. v. Union des consommateurs,
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/7e0u

[205] Plain Language Contract Act
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/fqg5

[206] Fordham Urban Law Journal, Volume 8, Number 2, 1979. Article 7, New York's Plain English Law. Rosemary Moukad
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/5s98

[207] New York Consolidated Laws, General Obligations Law - GOB § 5-702. Requirements for use of plain language in consumer transactions
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/xp8y

[208] LE CONTRAT D'ADHÉSION, Caractéristiques et Conséquences Juridiques. Luc Audet, avocat
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/dxjd

[209] Code civil du Québec annoté - Article 1379
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/j7sh

[210] Bakos, Yannis and Marotta-Wurgler, Florencia and Trossen, David R., Does Anyone Read the Fine Print? Consumer Attention to Standard Form Contracts (January 1, 2014). Journal of Legal Studies, Vol. 43, No. 1, 2014; CELS 2009 4th Annual Conference on Empirical Legal Studies Paper; NYU Law and Economics Research Paper No. 09-40.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/6fzg

[211] Cotton, H., & Bolan, C. (2011). User perceptions of end user license agreements in the smartphone environment.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/hajb

[212] Ben-Shahar, O. (2009). The Myth of the 'Opportunity to Read'in Contract law. European Review of Contract Law, 5(1), 1-28.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/x94m

[213] Ben-Shahar, O., & Schneider, C. E. (2011). The failure of mandated disclosure. University of Pennsylvania Law Review, 647-749.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/uf5h

[214] Ben-Shahar, O., & Schneider, C. E. (2014). More than you wanted to know: The Failure of Mandated Disclosure. Princeton University Press.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/402e

[215] Charte de la langue française
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/wbsn

[216] Google's MADA defines rules for Android device makers - Android Community
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/1foq

[217] How to Obtain Google's GMS License for Android Devices - Product Engineering Blog - IoT Blog - eInfochips
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/wpo1

[218] Google sued for MADA deals with smartphone makers, which made Android smartphones expensive - Latest Tech News, Video & Photo Reviews at BGR India
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/vqsf

[219] New Android OEM licensing terms leak; "Open" comes with a lot of restrictions - Ars Technica
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/ypxv

[220] Google's Dirty Little Android Secrets Leaked - Mobile - LinuxInsider
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/g30q

[221] Secret Ties in Google's 'Open' Android
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/l0ea

[222] Google 'Mobile Application Distribution Agreement' leaks, calls Android openness into question - Android Community
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/36ve

[223] Skyhook Google made OEMs break business deals, infringed patents - Ars Technica
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/nzzk

[224] Mahjoub (Re), 2016 CF 808 (CanLII)
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/ii5x

[225] R. c. Spencer, [2014] 2 RCS 212, 2014 CSC 43 (CanLII)
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/msbn

[226] R. c. Vu, [2013] 3 RCS 657, 2013 CSC 60 (CanLII)
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/bhsa

[227] R. c. Fearon, [2014] 3 RCS 621, 2014 CSC 77 (CanLII)
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/1t8p

[228] Virginia v. Baust No. CR141439 (Va. Cir. Ct. Oct. 28, 2014)
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/nb8a

[229] Court Rules Police May Compel Suspects to Unlock Fingerprint-Protected Smartphones, November 12, 2014
By Ken Winterbottom – Edited by Yixuan Long
Virginia v. Baust, No. CR14-1439 (Va. Cir. Oct. 28, 2014)
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/56h0

[230] Marc Sosna, Rosa Nelly Trevinyo-Rodríguez, S. Ramakrishna Velamuri, Business Model Innovation through Trial-and-Error Learning, Long Range Planning, Volume 43, Issue 2, 2010, Pages 383-407, ISSN 0024-6301, http://dx.doi.org/10.1016/j.lrp.2010.02.003.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/mswq

[231] Zott, C., Amit, R., & Massa, L. (2011). The business model: recent developments and future research. Journal of management, 37(4), 1019-1042.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/yv52

[232] Gritzalis D., Moulinos K., Kostis K. (2001) A Privacy-Enhancing e-Business Model Based on Infomediaries. In: Gorodetski V.I., Skormin V.A., Popyack L.J. (eds) Information Assurance in Computer Networks. MMM-ACNS 2001. Lecture Notes in Computer Science, vol 2052. Springer, Berlin, Heidelberg
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/lda1

[233] Dubosson-Torbay, M., Osterwalder, A. and Pigneur, Y. (2002), E-business model design, classification, and measurements. Thunderbird Int'l Bus Rev, 44: 5–23. doi:10.1002/tie.1036
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/28cz

[234] Osterwalder, A. (2004). The business model ontology: A proposition in a design science approach.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/kgh9

[235] Rappa, M. A. (2004). The utility business model and the future of computing services. IBM Systems Journal, 43(1), 32-42.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/qfs4

[236] O'Reilly, T. (2005). What is Web 2.0: Design patterns and business models for the next generation of software. Retrieved December 15, 2006.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/alk9

[237] Apple Inc's smartphone business model is Blackberry Ltd's opportunity - Financial Post
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/taxk

[238] OPPO Explained: How A Little-Known Smartphone Company Overtook Apple In China
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/g3f4

[239] iTunes' outdated business model is getting eaten alive
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/7vh8

[240] The iTunes Business Model and its Widespread Effects - The Vly House
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/6ers

[241] The Current I Tunes Business Model
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/x1bq

[242] Google Adsense Business Model
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/hnua

[243] Online Advertising Models CPC, CPM or CPA – Promise Media
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/htcp

[244] The End of Digital Advertising as We Know It - Knowledge@Wharton
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/w4xr

[245] Karolina Tutaj & Eva A. van Reijmersdal (2012) Effects of online advertising format and persuasion knowledge on audience reactions, Journal of Marketing Communications, 18:1, 5-18,
DOI: 10.1080/13527266.2011.620765
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/j3za

[246] Allan Afuah. Business Model Innovation: Concepts, Analysis, and Cases
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/tmwg

[247] Why Google Is Buying AdMob - Bloomberg
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/unn4

[248] Understanding App Monetization with Google AdMob - The Economic Times
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/wojx

[249] Economic Analysis of Business Model for Delivering Mobile Value Added Services in Thailand
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/68jk

[250] The Entire Business Model Of A Search Engine...' (Summarised In LESS THAN 23 Words) - Tony J. Carter - Client Acquisition - Pulse - LinkedIn
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/o11t

[251] Google's Toughest Search Is for a Business Model - The New York Times
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/5sqg

[252] Le modèle économique de Google - idneuf
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/eswf

[253] Mehta, A., Saberi, A., Vazirani, U., & Vazirani, V. (2007). Adwords and generalized online matching. Journal of the ACM (JACM), 54(5), 22.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/vvrs

[254] Analysing the AdWords business model - Culttt
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/xfvl

[255] The 9 types of online business models; which one do you use?
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/hdat

[256] The 11 Most Popular Online Business Models - Empire Flippers
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/skjb

[257] Internet Small Business Models
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/whhq

[258] The 5 Most Innovative New Online Business Models in 2010 - OPEN Forum
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/7mdf

[259] Sääksjärvi, M., Lassila, A., & Nordström, H. (2005, June). Evaluating the software as a service business model: From CPU time-sharing to online innovation sharing. In IADIS international conference e-society (pp. 177-186). Qawra, Malta.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/6apo

[260] Rappa, M. A. (2004). The utility business model and the future of computing services. IBM systems journal, 43(1), 32-42.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/zk50

[261] Robert G. Picard (2000) Changing business models of online content services: Their implications for multimedia and other content producers, International Journal on Media Management, 2:2, 60-68, DOI: 10.1080/14241270009389923
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/r3v3

[262] Audun Jøsang, Roslan Ismail, Colin Boyd, A survey of trust and reputation systems for online service provision, Decision Support Systems, Volume 43, Issue 2, 2007, Pages 618-644, ISSN 0167-9236,
http://dx.doi.org/10.1016/j.dss.2005.05.019.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/1oq2

[263] A. Ojala and P. Tyrvainen, "Developing Cloud Business Models: A Case Study on Cloud Gaming," in IEEE Software, vol. 28, no. 4, pp. 42-47, July-Aug. 2011.
doi: 10.1109/MS.2011.51
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/2xz5

[264] Khanagha, S., Volberda, H. and Oshri, I. (2014), Business model renewal and ambidexterity: structural alteration and strategy formation process during transition to a Cloud business model. R&D Manage, 44: 322–340. doi:10.1111/radm.12070
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/zdc0

[265] Saul J. Berman, Lynn Kesterson Townes, Anthony Marshall, Rohini Srivathsa, (2012) "How cloud computing enables process and business model innovation", Strategy & Leadership, Vol. 40 Issue: 4, pp.27-35,
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/v8co

[266] Saul J. Berman, Lynn Kesterson Townes, Anthony Marshall, Rohini Srivathsa, (2012) "How cloud computing enables process and business model innovation", Strategy & Leadership, Vol. 40 Issue: 4, pp.27-35,
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/v8co

[267] Erik Brynjolfsson, Paul Hofmann, and John Jordan. 2010. Cloud computing and electricity: beyond the utility model. Commun. ACM 53, 5 (May 2010), 32-34.
DOI : http://dx.doi.org/10.1145/1735223.1735234
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/ghnx

[268] Weinhardt, C., Anandasivam, A., Blau, B. et al. Bus. Inf. Syst. Eng. (2009) 1: 391. doi:10.1007/s12599-009-0071-2
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/bd1p

[269] Identity-as-a-Service (IDaaS) for Cloud App SSO + Security
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/7f09

[270] Zwattendorfer, B., Stranacher, K., & Tauber, A. (2013, August). Towards a federated identity as a service model. In International Conference on Electronic Government and the Information Systems Perspective (pp. 43-57). Springer, Berlin, Heidelberg.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/24mr

[271] Gopalakrishnan, A. (2009). Cloud computing identity management. SETLabs briefings, 7(7), 45-54.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/myc4

[272] M. Ates, S. Ravet, A. M. Ahmat and J. Fayolle, "An Identity-Centric Internet: Identity in the Cloud, Identity as a Service and Other Delights," 2011 Sixth International Conference on Availability, Reliability and Security, Vienna, 2011, pp. 555-560. doi: 10.1109/ARES.2011.85
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/as8u

[273] Emig C., Brandt F., Kreuzer S., Abeck S. (2007) Identity as a Service – Towards a Service-Oriented Identity Management Architecture. In: Pras A., van Sinderen M. (eds) Dependable and Adaptable Networks and Services. EUNICE 2007. Lecture Notes in Computer Science, vol 4606. Springer, Berlin, Heidelberg
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/e0iz

[274] Bhardwaj, S., Jain, L., & Jain, S. (2010). Cloud computing: A study of infrastructure as a service (IAAS). International Journal of engineering and information Technology, 2(1), 60-63.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/z18h

[275] Mell, P., & Grance, T. (2011). The NIST definition of cloud computing.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/n9df

[276] Dykstra, J., & Sherman, A. T. (2012). Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques. Digital Investigation, 9, S90-S98.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/wrc8

[277] Prodan, R., & Ostermann, S. (2009, October). A survey and taxonomy of infrastructure as a service and web hosting cloud providers. In Grid Computing, 2009 10th IEEE/ACM International Conference on (pp. 17-25). IEEE.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/r6v6

[278] Data sovereignty What it is and why it matters
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/2lfr

[279] De Filippi, P, McCarthy, S, 'Cloud Computing: Centralization and Data Sovereignty' European Journal for Law and Technology, Vol. 3 No. 2, 2012
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/oq8v

[280] Chinese borrowers told to post nude photos as collateral
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/3d9m

[281] Federal Court decision issued in the Globe24h.com matter – The CanLII Blog
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/mnxu

[282] Pure Storage. BIG DATA'S BIG FAILURE:
The struggles businesses face in accessing the information they need
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/virx

[283] bug reporting - Getting 'System program problem detected' pops up regularly after upgrade - Ask Ubuntu
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/8jti

[284] Happy Apps - Blog, August 15, 2015. Software Instrumentation - Balancing Data Collection and Impact on Performance
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/4vv8

[285] Jeffery C., Al-Gharaibeh J. (2015) Software Instrumentation and Data Collection. In: Writing Virtual Environments for Software Visualization. Springer, New York, NY Software Instrumentation and Data Collection - SpringerLink
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/qz6n

[286] Mozilla Crash Reporter - Firefox Help
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/um32

[287] Using Profiling Methods to Collect Performance Data from the Command Line
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/gkii

[288] Mesurer les performances avec le profileur intégré - Performance - MDN
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/e1t5

[289] Getting Insight Into Your Userbase - Inside Intercom
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/a8sf

[290] Identity Insights to go beyond Market Level to individual Level - LoginRadius
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/y6y4

[291] Social Media Demographics for Marketers - Sprout Social
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/ccep

[292] Juniper Networks - Introduction to Big Data: InfrastruCture and Networking Considerations.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/cj3v

[293] Cunningham, S. J. (1998, March). Providing internet reference service for the New Zealand Digital Library: gaining insight into the user base for a digital library. In Proceedings of the 10th International Conference on New Information Technology (pp. 27-34).
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/9yqu

[294] The Sarbanes-Oxley Act 2002
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/2rsp

[295] 15 CFR 30.2 - General requirements for filing Electronic Export Information (EEI). - US Law - LII - Legal Information Institute
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/jys6

[296] Export Administration Regulations (EAR)
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/8ieb

[297] Export Administration Regulations (EAR)
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/01wn

[298] What is ITAR and EAR compliance - Definition from WhatIs.com
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/et2o

[299] Canadian Response to the U.S. Sarbanes-Oxley Act of 2002 New Directions for Corporate Governance (PRB 05-37E)
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/kpvh

[300] spoliation destruction of documents can pose serious consequences in litigation
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/jaaj

[301] Koesel, Margaret M., Tracey L. Turnbull, and Daniel F. Gourash. "Spoliation of evidence: sanctions and remedies for destruction of evidence in civil litigation." American Bar Association, 2006.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/zq5j

[302] Bill C198 - Sarbanes-Oxley for Canada
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/0s1j

[303] SPOLIATION OF EVIDENCE IN ALL 50 STATES. MATTHIESEN, WICKERT & LEHRER, S.C.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/drom

[304] Dismissal as a Sanction for Spoliation of Evidence - Alerts & Newsletters - Holland & Knight
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/5quy

[305] Financial Transactions and Reports Analysis Centre of Canada - Guidance
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/o9bh

[306] How Facebook Uses Artificial Intelligence and What It Means for Marketers
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/0ycn

[307] Experience Google's machine learning on your own images, voice and text - Google Cloud Big Data and Machine Learning Blog _ Google Cloud Platform
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/bbts

[308] Google releases audio dataset for machine-learning research
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/invh

[309] How Google could fire up its smart home play - TechCrunch
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/s99y

[310] Najafabadi, M. M., Villanustre, F., Khoshgoftaar, T. M., Seliya, N., Wald, R., & Muharemagic, E. (2015). Deep learning applications and challenges in big data analytics. Journal of Big Data, 2(1), 1.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/5j5l

[311] Qiu, J., Wu, Q., Ding, G., Xu, Y., & Feng, S. (2016). A survey of machine learning for big data processing. EURASIP Journal on Advances in Signal Processing, 2016(1), 67.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/w62s

[312] Sébastien Gambs, Marc-Olivier Killijian, and Miguel Núñez del Prado Cortez. 2012. Next place prediction using mobility Markov chains. In Proceedings of the First Workshop on Measurement, Privacy, and Mobility (MPM '12). ACM, New York, NY, USA, Article 3, 6 pages.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/cfpr

[313] Automated behavioral and static analysis using an instrumented sandbox and machine learning classification for mobile security
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/0f65

[314] Facebook doesn't listen through your phone's mic -- except when it does - Computerworld
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/xm37

[315] Bienvenue dans Mon activité
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/z0za

[316] Privacy Assistant App Uses Machine Learning to Limit Smartphone Data Collection - FintekNews
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/rbbx

[317] Open science data - Wikipedia
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/o1jh

[318] Open Data Access Policies and Strategies in the European Research Area and Beyond
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/lf28

[319] Latanya Sweeney. 2013. Discrimination in online ad delivery. Commun. ACM 56, 5 (May 2013), 44-54.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/1a5i

[320] Paulos, E., Kim, S., & Kuznetsov, S. (2011). 10 The Rise of the Expert Amateur: Citizen Science and Microvolunteerism. From Social Butterfly to Engaged Citizen: Urban Informatics, Social Media, Ubiquitous Computing, and Mobile Technology to Support Citizen Engagement, 167.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/2jva

[321] Marcus Foth. From Social Butterfly to Engaged Citizen: Urban Informatics, Social Media ...
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/bg9l

[322] Kim, S., Mankoff, J., & Paulos, E. (2014). Reflecting the Current Practices of Technology Use in Volunteer Data Collection Activities on the Opportunities of Mobile Technology. Technical Report, CMU-HCII-14-107, Carnegie Mellon University.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/4b5y

[323] Sunyoung Kim, Jennifer Mankoff, and Eric Paulos. 2015. Exploring Barriers to the Adoption of Mobile Technologies for Volunteer Data Collection Campaigns. In Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15). ACM, New York, NY, USA, 3117-3126.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/tpnh

[324] Sunyoung Kim, Jennifer Mankoff, and Eric Paulos. 2013. Sensr: evaluating a flexible framework for authoring mobile data-collection tools for citizen science. In Proceedings of the 2013 conference on Computer supported cooperative work (CSCW '13). ACM, New York, NY, USA, 1453-1462.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/rpww

[325] Sunyoung Kim, Jennifer Mankoff, and Eric Paulos. 2014. Exploring the opportunities of mobile technology use in nonprofit organizations. In CHI '14 Extended Abstracts on Human Factors in Computing Systems (CHI EA '14). ACM, New York, NY, USA, 1939-1944.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/vrg0

[326] Why do all these phone apps need my information - Forums - CNET
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/tt2d

[327] Third-party websites are getting a lot of your personal data from your mobile apps
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/60p3

[328] Android Security Android Apps Collect Private User Data Research
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/5qq2

[329] What do your apps know about you - Security, data and privacy - Subject areas - Publishing and editorial - BCS - The Chartered Institute for IT
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/893w

[330] 100,000 Android Apps Collect Too Much Data, Security Firm Finds - Carbon Black
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/ctbf

[331] How many mobile apps collect data on users Oh ... nearly all of them • The Register
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/9yds

[332] Hackintosh Instructions, Hackintosh How To Guides Hackintosh.com
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/677q

[333] Des câbles Lightning qui se jouent de la protection d'iOS 7 - iGeneration
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/g844

[334] About Apple Digital AV Adapters for iPhone, iPad, and iPod touch - Apple Support
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/029s

[335] Trusted Computing for Mac OS X
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/bo8b

[336] Trusted Computing Module - Official Apple Support Communities
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/s2oq

[337] Companies Can't Legally Void the Warranty for Jailbreaking or Rooting Your Phone - Motherboard
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/7pyu

[338] Magnuson-Moss Warranty Act of 1975
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/37yo

[339] Apple rejects Opera Browser, not surprising, but still upsetting - Apple Gazette
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/nk13

[340] Almerica's Blog About Technology and Other Interesting Stuff Podcaster rejeceted because it duplicates iTunes functionality
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/bkle

[341] Daring Fireball The App Store's Exclusionary Policies
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/750000000

[342] Apple Rejects iPhone App As Competitive To iTunes - Slashdot
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/ssd0

[343] Mobile Device Management (MDM) Protocolvisité le 2017-07-01; http
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/a0yp

[344] NSA might be behind weakening of Android Random Number Generator problem
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/f5sc

[345] Latest Snowden revelation NSA sabotaged electronic locks - LA Times
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/pd8j

[346] CVE - CVE-2017-0144visité le 2017-07-01; http
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/leon

[347] The need for urgent collective action to keep people safe online Lessons from last week's cyberattack - Microsoft on the Issuesvisité le 2017-07-01; http
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/e043

[348] The NSA Is Hoarding Vulnerabilities - Schneier on Securityvisité le 2017-07-01; http
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/mppv

[349] CVE - CVE-2014-0160visité le 2017-07-01; http
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/51k5

[350] M. P. Ward, "The formal transformation approach to source code analysis and manipulation," Proceedings First IEEE International Workshop on Source Code Analysis and Manipulation, Florence, 2001, pp. 185-193.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/l0nf

[351] MathWorld Code Analysis
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/xu5q

[352] VDiscover large-scale vulnerability discovery using Machine Learningvisité le 2017-07-01; http
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/on4v

[353] MAST · GitHubvisité le 2017-07-01; http
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/40a6

[354] Smalley, S., & Craig, R. (2013, February). Security Enhanced (SE) Android: Bringing Flexible MAC to Android. In NDSS (Vol. 310, pp. 20-38).
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/dctd

[355] SELinux in Android Lollipop and Marshmallow
Stephen Smalley
Trusted Systems Research
National Security Agency
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/8rq8

[356] What is Google's position of rooting QFuse - Forums des produits Google
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/v1fn

[357] Google Security Engineer Explains Issues With Root and Android Pay in the XDA Forums
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/zbl4

[358] RIM Downplays BlackBerry 10 Delays - PCWorld
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/fzyp

[359] The Rise And Fall Of Blackberry In One Big Graphic - Business Insider
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/nbxe

[360] Apple iPhone closing in on BlackBerry market share
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/c3ql

[361] The Agony of 'BlackBerry Thumb' - WIRED
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/iygq

[362] The agony of dying gadgets - The Spectator
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/kfuj

[363] The 11 moments that defined BlackBerry's rise and fall - TechRadar
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/1ufq

[364] Not even Google's Android can pull BlackBerry out of its tailspin - CNET
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/ncmb

[365] Access and Identity Management Solutions - Microsoft
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/y1sj

[366] Introducing Windows CardSpace
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/eagp

[367] THE RISE AND FALL OF BETA
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/3467

[368] Mer Project
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/8uud

[369] Native Application - Tizen Developers
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/b4gb

[370] Inglesant, P. G., & Sasse, M. A. (2010, April). The true cost of unusable password policies: password use in the wild. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (pp. 383-392). ACM.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/dgq5

[371] Mujeye, S., & Levy, Y. (2013). Complex passwords: How far is too far? The role of cognitive load on employee productivity. Online Journal of Applied Knowledge Management, 1(1), 122-132.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/cukm

[372] Horcher, A. M., & Tejay, G. P. (2009, June). Building a better password: The role of cognitive load in information security training. In Intelligence and Security Informatics, 2009. ISI'09. IEEE International Conference on (pp. 113-118). IEEE.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/w5td

[373] Singer, A., Anderson, W., & Farrow, R. (2013). Rethinking password policies. uncut): https://www. usenix. org/publications/login, 38.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/qlm5

[374] Brooks, R. R. (2013). Introduction to Computer and Network Security: Navigating Shades of Gray. CRC Press.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/cvcc

[375] L'infâme Laubardemont disait un jour Qu'on me donne six lignes écrites de la main du - Dicocitations & Le Monde
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/0gok

[376] We are Anonymous. We do not forgive. We do not forget - Dazed
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/c151

[377] Information and Response to the Ashley Madison Hack and List Leak
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/at9t

[378] Understanding Permissions
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/7euc

[379] TrustedBSD - TrustedBSD Mandatory Access Control (MAC) Frameworkvisité le 2017-07-01; http
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/ttdf

[380] Modèle OSI — Wikipédia
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/b6if

[430] Catégorie # 54, Message #124489, Forum FireFly de Anatol's Atol, Darknet
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/glu7

[431] Catégorie # 54, Message #120529, Forum FireFly de Anatol's Atol, Darknet
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/d09a

[381] Recueil de notes MIG9250, Méthodologie de recherche. Martin Cloutier. (2013)
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/5wyv

[382] Smart contract - Wikipedia
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/7tvq

[383] Manuel du cours EDP 1001 (Université de Montréal), Ibrahima Seye
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/9z93

[384] Economics and Computation. David C. Parkes et Sven Seuken. Inédit.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/ebgh

[385] Welcome to Tor Metrics
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/0t7e

[386] Dark Net Markets Are Booming From Better Quality & Safety
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/54km

[387] The NSA Is Scaring People Away From Tor
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/fzhm

[388] FBI Harassing Core Tor Developer, Demanding She Meet With Them, But Refusing To Explain Why - Techdirt
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/1r5t

[389] A Primer on DarkNet Marketplaces — FBI
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/vcm0

[390] The NSA Wants You to Trust Tor, Should You
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/pjo9

[391] Oversight of the Federal Bureau of Investigation — FBI
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/n0ev

[392] "Digital Refugee" The Impact of Technology on Syrian Migrants and The Smugglers Who Profit – Technology and Operations Management
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/k9jt

[393] How Google Search Usage Patterns Can Reflect the Path and Timing of Migrant Flows from the Middle East to Europe - Pew Research Center
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/8ybg

[394] Tor takes anonymity mobile with new smartphone OS - The Daily Dot
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/l3xn

[395] What is a Burner Phone And How Do They Work
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/0ykr

[396] Rosenberg, J. B., & Remy, D. L. (2004). Securing Web Services with WS-Security: Demystifying WS-Security, WS-Policy, SAML, XML Signature, and XML Encryption. Sams.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/bshu

[397] How much is a user worth - evaluating company worth due to user base
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/bun9

[398] Louis, T. (2013). How much is a user worth. 2016-O3-23).
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/jfob

[399] attacks - Can webcams be turned on without the indicator light - Information Security Stack Exchange
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/330e

[400] Errata Security How to disable webcam light on Windows
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/ztos

[401] Zhu, Z., & Cao, G. (2013). Toward privacy preserving and collusion resistance in a location proof updating system. IEEE Transactions on Mobile Computing, 12(1), 51-64.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/b35t

[402] A Secure Anti-Collusion Data Sharing Scheme for Dynamic Groups in the Cloud – Ch.Ramesh Kumar, B.Prasanna Jyothi & Ireni Sathish Goud
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/d961

[403] Your privacy at airports and borders - Office of the Privacy Commissioner of Canada
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/0un6

[404] What Are Your Rights if Border Agents Want to Search Your Phone - The New York Times
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/2660

[405] Access Yahoo email from another country - Web Applications Stack Exchange
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/ptb3

[406] Trusted third party - Wikipedia
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/jjsz

[407] The components of the Integrated Electronic Consular System (E-Cons)
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/h8fe

[408] Death abroad - Travel.gc.ca
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/hhu5

[409] Mattke, J., Müller, L. K., & Maier, C. (2017). Why do individuals block online ads? An explorative study to explain the use of ad blockers.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/mpix

[410] Datta, B., & Madio, L. (2017). E ects of Ad-Blockers Adoption on Digital Piracy: A Blessing or a Curse?.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/5cy9

[411] Tails - Confidentialité et anonymat, pour tout le monde et partout
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/480t

[412] Libertarianism (Stanford Encyclopedia of Philosophy)
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/pm15

[413] February 16, 2016, US Magistrate Judge Sheri
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/xkfv

[414] How to Add an Emergency Contact to Your Phone's Lock Screen - PCMag.com
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/gp66

[415] Let's Encrypt Stats - Let's Encrypt - Free SSL_TLS Certificates
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/i99v

[416] Rapport annuel sur la surveillance électronique - 2013
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/kl2z

[417] Krippendorff, K. (2004). Content analysis: An introduction to its methodology. Sage.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/2cve

[418] Martin L. Cloutier. Manuel du cours MIG9100.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/ojbh

[419] Aceto, S., Delrio, C., Dondi, C., Fischer, T., Kastis, N., Klein, R., ... & Corbin, J. (1994). Grounded theory methodology-An overview. Handbook of qualitative research. Thousand Oaks: Sage Publications.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/h7f1

[420] Dohnal, M. (1991). A methodology for common-sense model development. Computers in Industry, 16(2), 141-158.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/aafd

[421] Bresciani, P., Perini, A., Giorgini, P., Giunchiglia, F., & Mylopoulos, J. (2004). Tropos: An agent-oriented software development methodology. Autonomous Agents and Multi-Agent Systems, 8(3), 203-236.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/cis0

[422] Nance, R. E. (1994). The conical methodology and the evolution of simulation model development. Annals of operations research, 53(1), 1-45.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/nv5q

[423] Lee, S. D., Yang, Y. J., Cho, F. S., Kim, S. D., & Rhew, S. Y. (1999). COMO: A UML-based component development methodology. In Software Engineering Conference, 1999.(APSEC'99) Proceedings. Sixth Asia Pacific (pp. 54-61). IEEE.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/0cqv

[424] Leem, C. S., Jeon, N. J., Choi, J. H., & Shin, H. G. (2005, May). A business model (BM) development methodology in ubiquitous computing environments. In International Conference on Computational Science and Its Applications (pp. 86-95). Springer, Berlin, Heidelberg.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/3qd8

[425] Biggest Apple Account Theft Ever Hits Only
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/alew

[426] An Experimental Study on the Role of Password Strength and Cognitive Load on Employee Productivity
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/tpc2

[427] What Is the 'Reasonable Expectation of Privacy'
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/vr6r

[428] Apple's battle with the FBI leaves lingering questions - CNET
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/tlkl

[429] Catégorie # 54, Message #123523, Forum FireFly de Anatol's Atol, Darknet
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/j5f3

[432] Youn, S. (2009). Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents. Journal of Consumer affairs, 43(3), 389-418.
récupéré le 2017-07-01, depuis : http://uu1.ca/cite/xttc/5qfk