Université de Montréal

La surveillance financière à l'ère du Big Data : L'implantation d'outils algorithmiques dans le cadre de la lutte au blanchiment d'argent et au financement du terrorisme

Par Maude Dufour

École de Criminologie
Faculté des Arts et des Sciences

Travail dirigé présenté à la Faculté des études supérieures et postdoctorales en vue de l'obtention du grade de *Maîtrise ès sciences* (M. Sc.)
En Criminologie
Option Sécurité intérieure

Décembre 2019

Remerciements

Je tiens tout d'abord à remercier mon directeur de recherche, Anthony Amicelle, pour son soutien tout au long de cette recherche. Ses judicieux conseils et son expertise ont été déterminants dans le cadre de cette étude.

J'aimerais également remercier la banque pour son accord quant à la participation à cette recherche ainsi que les personnes qui ont contribué aux entrevues. Leur participation et le partage de leurs expériences ont été fondamentaux pour la réalisation de cette recherche.

Un merci particulier à ma famille qui m'a encouragée dans le cadre de mes études universitaires. Plus spécifiquement, merci à mes parents pour leur soutien considérable et toute l'aide qu'ils ont pu m'offrir.

Je remercie également mes amis qui ont su me divertir et me changer les idées lorsque nécessaire, mais qui ont aussi été compréhensifs à l'égard de mon indisponibilité.

Je tiens aussi à remercier mes collègues de travail pour leurs continuels encouragements tout au long de la rédaction.

Enfin, je tiens à remercier mes collègues à la maîtrise avec lesquels il a été possible de mutuellement partager nos nombreuses remises en question et nos doutes. À maintes reprises, il a été possible de se faire part des critiques et de nos inquiétudes face à la rédaction. À ces heures interminables passées à la bibliothèque et ces quelques pauses bien méritées !

Résumé

Les banques se retrouvent aujourd'hui en première ligne en ce qui a trait à la lutte au blanchiment d'argent et au financement du terrorisme. Alors qu'elles doivent surveiller des milliers, voire des millions de transactions financières chaque jour, il devient difficile pour les banques de détecter les transactions potentiellement suspectes. Par conséquent, des algorithmes sont utilisés à des fins de détection automatisée, une pratique courante à l'ère du *Big Data* dans le domaine de la sécurité et plus particulièrement de la surveillance. Ainsi, la présente recherche s'est intéressée à l'implantation d'un outil algorithmique au sein d'une banque canadienne, et ce, dans le cadre de la lutte au blanchiment d'argent et financement du terrorisme. Pour ce faire, des entretiens semi-dirigés ont été réalisés auprès de huit personnes qui travaillent au sein de cette banque. Les résultats de la recherche ont mis de l'avant les changements survenus en matière de surveillance à la suite de l'implantation de l'outil.

Mots clés : Blanchiment d'argent, financement du terrorisme, banques, institutions financières, surveillance financière, renseignement financier, nouvelles technologies, Big Data, algorithmes, instruments de sécurité, implantation.

Abstract

Today, banks are the first line of defence in the fight against money laundering and financing of terrorism. Banks have to monitor thousands or even millions of financing transactions every day, which makes it difficult for them to detect potentially suspicious transactions. Therefore, banks utilize algorithms, which is a common practice in the security realm more especially in surveillance, as automatized detection means. This research focuses on an algorithm device implantation in a Canadian bank used in the fight against money laundering and financing of terrorism. Semi-structured interviews were conducted with eight individuals working for that bank. The results of the research put forward the changes in surveillance after the device implantation.

Keywords : Money laundering, financing of terrorism, banks, financial institutions, financial surveillance, financial intelligence, new technologies, Big Data, algorithms, security devices, implantation.

TABLE DES MATIÈRES

Introduction.....1
Chapitre 1 – Revue de la littérature.....3
1. La lutte au blanchiment d'argent et au financement du terrorisme.....3
1.1. Le blanchiment d'argent.....3
1.1.1. De la Guerre contre la drogue à la création du blanchiment d'argent.....3
1.1.2. Le blanchiment d'argent : un enjeu à l'échelle internationale.....6
1.2. Le financement du terrorisme.....7
1.2.1. L'ère post 9/11 : le financement du terrorisme, un fondement à la lutte.....7
1.2.2. Les législations à l'égard du financement du terrorisme.....9
1.3. La surveillance des flux financiers.....11
1.3.1. Les banques : « des sentinelles de l'argent sale » 11
1.3.2. Les critiques associées à la surveillance financière.....14
2. Les nouvelles technologies de surveillance.....18
2.1. Les pratiques en matière de surveillance.....18
2.1.1. L'émergence du Big Data : la solution aux problèmes de sécurité.....18
2.1.2. L'utilisation des algorithmes dans le domaine de la sécurité.....20
2.1.3. Préoccupations légales et techniques.....22
2.2. La technologie au sein des organisations de *policing* : les impacts.....25
2.2.1. L'implantation de nouvelles technologies.....25
2.2.2. Les transformations au sein des pratiques.....27
2.2.3. Les défis d'implantation auxquels les organisations sont confrontées.....28
Chapitre 2 – Problématique.....32
Chapitre 3 – Cadre théorique.....34
Chapitre 4 – Méthodologie.....36
1. La méthodologie qualitative.....36
2. La collecte de données.....37
3. Les limites méthodologiques.....38

Chapitre 5 – Analyse des résultats.....40
1. La formulation de l'instrument.....40
1.1. Le processus de décision : les motivations à l'égard de l'implantation.....40
1.2. Le processus de sélection de l'instrument : le choix du logiciel.....42
1.3. La conception de l'outil : la paramétrisation.....43
2. La mise en œuvre de la technologie au sein de la banque.....46
2.1. La préparation à l'implantation d'une nouvelle technologie.....46
2.2. L'introduction de la technologie.....49
2.3. Les enjeux associés à l'implantation d'une nouvelle technologie.....50
3. L'appropriation de la technologie par les utilisateurs.....52
3.1. Les pratiques de surveillance algorithmique.....52
3.2. Les enjeux de l'appropriation de la technologie.....55
Chapitre 6 – Discussion.....57
Conclusion.....64
Bibliographie.....67

INTRODUCTION

L'argent sale est aujourd'hui perçu comme un enjeu à l'échelle mondiale : d'une part, l'argent issu d'activités criminelles et, d'autre part, l'argent destiné à la commission d'actes terroristes, représentent une menace. En effet, le blanchiment d'argent est considéré comme préoccupant quant aux conséquences sur les systèmes financiers légitimes et les avantages procurés aux criminels, suscitant une mobilisation internationale (Gilmore, 2011 ; Stessen, 2000 ; Canafe, 2019). Parallèlement, le terrorisme est perçu comme une menace à la sécurité nationale et internationale, engendrant la mise en place de plusieurs mesures antiterroristes, dont certaines s'attaquant plus spécifiquement aux fonds terroristes. À cet effet, s'attaquer à la source du terrorisme, soit le financement, est considéré comme un fondement dans la lutte au terrorisme, dans l'optique où l'élimination des fonds permettrait d'empêcher, ou du moins de limiter, les actes terroristes (Amicelle, 2008 ; Biersteker et Eckert, 2008). Ainsi, la lutte au financement du terrorisme s'est jointe à la lutte au blanchiment d'argent, lesquelles sont aujourd'hui exercées conjointement.

À cet égard, la lutte à l'argent sale se situe à la fois dans le domaine de la sécurité et celui de la finance, et place par conséquent les banques en première ligne en ce qui a trait à la surveillance des flux financiers (Amicelle, 2018 ; Favarel-Garrigues, Godefroy et Lascoumes, 2009). De ce fait, les banques sont assujetties à de nouvelles obligations, requérant plusieurs changements au sein des organisations, dont entre autres des réorganisations internes et l'implantation d'outils technologiques destinés à les supporter (Favarel-Garrigues, Godefroy et Lascoumes, 2009 ; Amicelle, 2008). Bien que les banques se dotent de plus en plus de ces nouvelles technologies, aucune recherche empirique ne s'est attardée à leur utilisation et leur implantation au sein des banques. Parallèlement, plusieurs écrits scientifiques ont abordé les pratiques liées au *Big Data* et l'utilisation des technologies de surveillance et des algorithmes dans le domaine de la sécurité. Par contre, très peu d'écrits portent sur l'utilisation, par les banques, des algorithmes à partir du *Big Data*, alors qu'elles ont des milliers, voire des millions de transactions financières à surveiller chaque jour (Roberge, 2004 ; Amicelle, 2019). De surcroît, la littérature portant sur la surveillance et les algorithmes est principalement théorique et peu basée sur des

données empiriques. Par conséquent, il s'avère opportun de s'intéresser à l'utilisation et à l'implantation d'outils algorithmiques afin de réellement comprendre les pratiques de surveillance dans le cadre de la lutte à l'argent sale au sein des banques.

Ainsi, cette recherche s'intéresse à l'implantation d'un outil algorithmique au sein d'une banque canadienne et vise plus précisément à comprendre de quelles façons cet outil modifie la surveillance dans le cadre de la lutte au blanchiment d'argent et au financement du terrorisme : Quels sont les défis ? ; Quels sont les impacts ? ; Comment les pratiques changent-elles ? ; Quelles sont les résistances lors de l'implantation ? Cette recherche vise également à combler les lacunes dans la littérature, et ce, à partir de données empiriques. La présente recherche est donc divisée en 6 chapitres, soit la revue de la littérature, la problématique, le cadre théorique de la recherche, la méthodologie, l'analyse des résultats et la discussion, suivis d'une conclusion.

CHAPITRE 1 – REVUE DE LA LITTÉRATURE

1. La lutte au blanchiment d'argent et au financement du terrorisme

1.1 Le blanchiment d'argent

1.1.1. De la Guerre contre la drogue à la création du blanchiment d'argent

Durant les années 1960 et 1970, la production et le trafic de drogues sont considérés comme une menace à la sécurité nationale et deviennent un enjeu prioritaire pour les États-Unis (Gilmore, 2011 ; Amicelle, 2017). À cet effet, la Guerre aux drogues déclarée en 1969 par le président américain Richard Nixon augmente l'attention portée à la criminalité organisée, qui devient désormais directement reliée au trafic de stupéfiants (Gilmore, 2011 ; Amicelle, 2017 ; Favarel-Garrigues, Godefroy et Lascoumes, 2009). Parallèlement, dans les années 1970 et 1980, la menace posée par la criminalité transnationale devient une préoccupation de plus en plus importante aux yeux du public et se place dès lors au sein de l'agenda politique (Gilmore, 2011). À cet égard, la mondialisation et l'avènement de nouvelles technologies facilitent la communication à l'international et facilitent l'envoi d'argent à faibles coûts rapidement et facilement, et ce, à travers le monde (Nance, 2018a ; Gilmore, 2011 ; Foumdjem, 2011 ; Roberge, 2004). Ces circonstances, jointes à l'arrivée des « banques modernes », favorisent le commerce transnational, fournissant ainsi de nouvelles opportunités de marché pour les criminels (Gilmore, 2011 ; Foumdjem, 2011 ; Roberge, 2004). La criminalité organisée et transnationale reliée au trafic de stupéfiants génère donc des gains économiques faramineux pour ces criminels, lesquels sont perçus comme une menace à la stabilité économique et politique (Stessens, 2000). Conséquemment, les États amorcèrent l'adoption de différentes législations afin d'intervenir à l'égard du trafic de drogues (Stessens, 2000). Concurremment, l'Organisation des Nations Unies (ONU) entreprit la mise en place de conventions afin de contrôler l'abus et le trafic de stupéfiants, qui devenaient indéniablement nécessaires d'être contrôlés à l'international (Gilmore, 2011). Les premières mobilisations nationales et internationales en ce qui a trait au blanchiment d'argent ciblaient donc principalement les

trafiquants de stupéfiants (Roberge, 2004). Éventuellement, cette succession d'évènements et le contexte les entourant ont finalement résulté en la création d'un nouveau crime, soit le blanchiment d'argent. Bien que ce terme était déjà utilisé auparavant, il ne s'agissait pas d'un crime. Ainsi, les États-Unis furent les premiers à promulguer une loi sur le blanchiment d'argent en 1986 (Amicelle, 2017 ; Nance, 2018a). Les États ont donc commencé à être conscientisés quant aux conséquences néfastes du blanchiment d'argent sur le système financier et considèrent dès lors ce dernier comme un problème public (Gilmore, 2011). En revanche, certains auteurs relatent que le problème de « *criminal money management* », plus tard appelé blanchiment, n'est ni un phénomène nouveau, ni une nouvelle menace des années 1970 et 1980 (Van Duyne, Harvey et Gelemerova, 2018). De plus, Van Duyne, Harvey et Gelemerova (2018) soulignent que bien que les délégués des États aient exprimé leur « *grave concern* » à l'égard du blanchiment d'argent issu du trafic de stupéfiants, cette préoccupation serait plutôt le résultat d'une association opportune : l'accroissement du trafic de drogues dans les années 1980 fut associé au blanchiment d'argent, entraînant l'idée d'une menace sérieuse au système financier. Toutefois, après un quart de siècle, ces auteurs soulèvent que cette menace n'a toujours pas été confirmée (Van Duyne, Harvey et Gelemerova, 2018).

Alors que la lutte au blanchiment d'argent s'insère en premier lieu dans le cadre de la Guerre contre la drogue, aujourd'hui cette lutte a élargi son champ d'action à d'autres activités criminelles, notamment le trafic humain et le trafic d'armes (Scura, 2013 ; Levi, 2002). Scura (2013) définit le blanchiment d'argent comme étant : « The process by which one conceals the existence, illegal source, or illegal application of income, and then disguises that income to make it appear legitimate » (p.1270). Il s'agit donc de gains économiques qui découlent d'activités criminelles, *proceeds of crime* (Levi et Reuter, 2006). À cet effet, Levi (2002) souligne qu'il est important, voire primordial de s'intéresser au blanchiment d'argent, puisqu'il dissimule des *proceeds of crime* du trafic de drogues certes, mais également de crimes graves. Or, cet argent gagné de façon illicite doit être blanchi, ce qui est habituellement fait par le biais de trois étapes : le placement, l'empilage et l'intégration. Tout d'abord, l'argent sale est placé dans une entreprise légitime ou une banque, où les fonds sont ensuite répartis en plusieurs transactions afin de masquer la

source. Finalement, les fonds blanchis sont intégrés dans le système financier légitime de différentes façons et semblent désormais avoir une apparence licite (Scura, 2013 ; Chappez, 2003 ; Gilmore 2011).

Ainsi, tel que souligné par Gilmore (2011), le blanchiment d'argent peut avoir des répercussions sur l'économie mondiale en nuisant aux opérations des économies nationales risquant de corrompre lentement le marché financier, résultant ainsi en une perte de confiance du public envers le système financier (Stessens, 2000). De ce fait, les risques et les instabilités de ce système augmentent et peuvent réduire le taux de croissance de l'économie mondiale (Gilmore, 2011). Cependant, Van Duyne, Harvey et Gelemerova (2018) relatent qu'il y a un manque d'études sur les perturbations du système financier causé par le blanchiment d'argent. De plus, ils mentionnent qu'il s'agit uniquement de suppositions sur les sommes d'argent blanchi, étant donné qu'il est impossible de réellement connaître le montant de ces sommes ; de même en ce qui a trait à la gravité du problème, laquelle demeure incertaine (Van Duyne, Harvey et Gelemerova, 2018). Ainsi, ils soulignent que la menace posée par le blanchiment d'argent est peu supportée par des faits empiriques (Van Duyne, Harvey et Gelemerova, 2018).

Par ailleurs, Van Duyne, Harvey et Gelemerova (2018) mettent de l'avant que lorsqu'un « *grave concern* » est continuellement exprimé par les dirigeants mondiaux, il est alors prévisible de s'attendre à ce que la communauté politique internationale apporte son soutien. Par conséquent, à la fin des années 1980, le blanchiment d'argent, qui était dès lors perçu politiquement comme un crime financier devant être géré au niveau national, devint un enjeu sur le plan international (Amicelle, 2008 ; Svedberg Helgesson et Mörth, 2012 ; Foumdjem, 2011). De ce fait, la lutte au blanchiment d'argent doit se faire de concert avec les États, notamment par le biais d'organisations internationales qui permettent la diffusion de standards internationaux. Cette diffusion permet entre autres une conformité au sein des législations nationales (Foumdjem, 2011 ; Favarel-Garrigues, Godefroy et Lascoumes, 2009).

1.1.2. Le blanchiment d'argent : un enjeu à l'échelle internationale

De nombreux traités et législations se sont indirectement attaqués au blanchiment d'argent. Effectivement, les Nations Unies, dans une perspective de Guerre à la drogue, ont adopté certains traités, notamment le *UN Single Convention on Narcotic Drugs* de 1961 et le *UN Convention on Psychotropic Substances* de 1971. Bien que ces traités aient eu une contribution dans la lutte au trafic de stupéfiants, ils n'étaient pas adéquats pour gérer le trafic international de stupéfiants (Gilmore, 2011). En 1988, le *UN Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances* fut mis en place. Gilmore (2011) souligne que ce traité constitue la fondation d'un régime légal fort important dans le domaine, lequel concerne également le blanchiment d'argent. Il s'agit donc du premier instrument universel définissant le blanchiment de capitaux, sans toutefois employer le terme (Foumdjem, 2011 ; Van Duyne, Harvey et Gelemerova, 2018). Ces progrès facilitent ainsi la coordination des actions internationales contre le blanchiment d'argent issu de la criminalité (Gilmore, 1992). Ces textes initiaux vont donc éventuellement mener à la mise en place de mesures portant explicitement sur le blanchiment d'argent.

Ainsi, alors que les 7 pays les plus industrialisés se réunissaient à Paris en 1989 dans le cadre du Sommet du G7[1], une structure intergouvernementale fut créée : le Groupe d'Action Financière (GAFI)[2] (Amicelle, 2008 ; Gilmore, 2011). Selon Van Duyne, Harvey et Gelemerova (2018), le GAFI est un « club informel » créé par ce « groupe informel » composé de 7 dirigeants ; ayant pour objectif de lutter contre le blanchiment d'argent, et ce, notamment par l'élaboration de normes (Nance, 2018a). À cet effet, Scherrer (2006) souligne qu'initialement, le mandat du GAFI s'inscrivait uniquement dans une lutte au blanchiment d'argent relié au trafic de stupéfiants, alors qu'aujourd'hui, de nouvelles activités se sont jointes au mandat. Ainsi, en 1990, le GAFI a élaboré 40 recommandations afin de lutter contre le blanchiment d'argent, qui portaient sur trois aspects majeurs : l'amélioration du système légal national, le renforcement du rôle du système financier et

[1] Il s'agit d'un groupe composé des 7 pays les plus industrialisés : Canada, France, Allemagne, Italie, Japon, Royaume-Uni et États-Unis.

[2] Initialement composé des pays membres du G7, de la Commission Européenne et des pays suivants : Pays-Bas, Belgique, Luxembourg, Espagne, Suisse, Autriche, Australie et Suède. (GAFI, s.d.)

le renforcement de la coopération internationale. Les États étaient dès lors fortement invités à appliquer ces standards établis par le GAFI (Roberge, 2011 ; Gilmore, 2011 ; Nance, 2018a). Bien que le GAFI fut créé par le G7, plusieurs États[3] se sont joints à cet organisme intergouvernemental ; cette lutte devant être effectuée en collaboration avec les États (Nance, 2018a). De plus, malgré le fait que le GAFI émette des standards internationaux, les États ont tout de même la possibilité de définir les enjeux moraux de la lutte contre le blanchiment d'argent, selon leurs intérêts nationaux (Favarel-Garrigues, 2005a). « La liste des infractions initiales dont les produits sont susceptibles d'être blanchis peut donc considérablement varier d'un pays à un autre. » (Favarel-Garrigues, 2005a, p.576).

D'autant plus, le GAFI s'associe avec différents organismes internationaux dans l'exercice de ses fonctions. De fait, le Fond Monétaire International (FMI) et la Banque Mondiale collaborent avec le GAFI dans l'application des standards (Favarel-Garrigues, 2005b. ; Roberge, 2004). À cet égard, le FMI a joué un rôle fort important dans la lutte au blanchiment d'argent à l'échelle mondiale par sa coopération avec le GAFI dans l'évaluation de la mise en œuvre des recommandations et par sa contribution au développement des politiques (Kyriakos-Saad, Esposito et Schwarz, 2012). Par ailleurs, « L'engagement actif du FMI et de la Banque mondiale dans la lutte contre l'argent sale représente l'un des principaux effets des évènements de 2001 au niveau institutionnel » (Favarel-Garrigues, Godefroy et Lascoumes, 2009). Ainsi, Favarel-Garrigues (2005b) soulève que l'attention portée au financement du terrorisme suite au 11 septembre 2001 aura contribué par le fait même à accentuer les mesures prises en matière de lutte antiblanchiment.

1.2. Le financement du terrorisme

1.2.1. L'ère post 9/11 : le financement du terrorisme, un fondement à la lutte

Depuis les dernières années, le terrorisme prend une place indéniable au sein de l'agenda politique : le terrorisme menace les démocraties et la sécurité nationale et internationale. L'attention considérable qui est aujourd'hui portée au terrorisme, s'est bien évidemment

[3] Aujourd'hui 36 pays et territoires sont membres et 2 organisations régionales (Commission Européenne et Conseil de Coopération du Golfe) (GAFI, s.d.).

intensifiée au lendemain des attentats terroristes du 11 septembre 2001 (Banifatemi, 2002). George W. Bush, président des États-Unis, déclara la guerre au terrorisme et invita les États à prendre des mesures efficaces à l'échelle nationale, en plus de solliciter la collaboration des États au niveau international (Biersteker et Eckert, 2008). Par contre, le terrorisme n'est assurément pas un phénomène nouveau, contrairement à l'attention qui lui est désormais portée ; une convention avait été créée en 1999, la *Convention internationale pour la répression du financement du terrorisme de 1999*, laquelle avait été ratifiée par seulement 4 pays lors du 11 septembre 2001 (Biersteker et Eckert, 2008 ; Amicelle, 2011). Ainsi, étant aujourd'hui décelé comme problème public, des efforts sont déployés et des ressources financières sont affectées, afin de contrer le terrorisme. À cet égard, lutter contre le financement du terrorisme constitue l'une des principales mesures de contreterrorisme (Amicelle, 2008). En effet, selon Biersteker et Eckert (2008), s'attaquer au financement du terrorisme s'avère être l'un des fondements de la lutte au terrorisme, où limiter les ressources disponibles peut prévenir la mise en place d'attaques, ou du moins, réduire l'impact des attaques qui n'ont pu être prévenues (Banifatemi, 2002). D'autant plus, Johnson et Jensen (2010) soulignent que suivre l'argent peut permettre d'identifier celui qui envoie l'argent certes, mais également celui qui le reçoit. Par conséquent, il devient possible d'identifier des membres d'une cellule terroriste. De plus, Bures (2012) souligne que s'attaquer au financement du terrorisme est aussi d'utilité politique, étant donné qu'il est question de mesures concrètes, ce qui démontre au public que des actions sont mises en place afin de contrer le terrorisme et d'assurer leur sécurité (Marron, 2008).

Toutefois, il est difficile de suivre l'argent destiné au financement du terrorisme, puisqu'il peut s'agir d'infimes montants, dont la somme ne soulève aucun soupçon (Bierseker et Eckert, 2008 ; Nance, 2018a). Effectivement, la commission d'actes terroristes ne nécessite pas d'exorbitantes sommes d'argent (Roberge, 2004). D'ailleurs, malgré l'ampleur des attentats terroristes de 2001, il n'aurait suffi que de 400 000$ à 500 000$ pour réaliser ces attaques (Bierseker et Eckert, 2008). De plus, le financement peut provenir de sources illégales (la commission de crimes), mais également de sources légales (des fonds provenant de charités, de mosquées, de collectes de fonds, etc.) (Bierseker et Eckert, 2008 ; Amicelle, 2008 ; Roberge, 2004). De surcroît, Johnson et Jensen (2010) mentionnent que

les terroristes, étant constamment sous surveillance, ne cessent d'innover quant aux moyens utilisés pour le transfert de fonds servant au financement d'activités terroristes, notamment par l'envoi de plusieurs petites sommes d'argent et l'utilisation de systèmes financiers informels, rendant plus complexe la lutte au financement du terrorisme.

Par ailleurs, au lendemain des attentats terroristes de 2001, étant dépourvu de mesures visant à lutter contre le financement du terrorisme, les mesures d'antiblanchiment d'argent furent utilisées à cet effet par les différents acteurs du milieu (Amicelle, 2008 ; Foumdjem, 2011). Toutefois, Levi (2010) et Roach (2011) soulignent qu'il est difficile d'appliquer congrûment les mesures d'antiblanchiment d'argent au financement du terrorisme : les mesures visant à lutter contre le blanchiment d'argent visent des montants d'argent importants, alors que le terrorisme est souvent financé par de faibles sommes d'argent. De plus, alors que l'argent blanchi provient de la commission de crimes, l'argent destiné au financement du terrorisme peut provenir autant de sources illégitimes que légitimes (Amicelle, 2008 ; Foumdjem, 2011). Enfin, bien qu'il existe des différences fondamentales entre les deux, la lutte au blanchiment d'argent et au financement du terrorisme se font aujourd'hui conjointement, ce qui n'était pas le cas auparavant.

1.2.2. Les législations à l'égard du financement du terrorisme

Les évènements du 11 septembre 2001 ont intensifié l'intérêt porté au terrorisme et ont engendré une multiplication des mesures de contreterrorisme, nonobstant le caractère plutôt archaïque du terrorisme. De fait, les dispositions mises en œuvre, à la suite de ces évènements, ne sont pas les premières à légiférer contre le terrorisme. En effet, en 1999, des sanctions antiterroristes furent imposées par l'Organisation des Nations Unies, pour la première fois, directement vers un gouvernement. Effectivement, la résolution 1267, créée en 1999 concevait un Comité, lequel créa une liste de sanctions, et exigeait le gel de fonds et des ressources du gouvernement Afghan (les Talibans) (Johnson et Jensen, 2010 ; Cameron, 2003 ; de Goede, 2011). Le lendemain des attaques terroristes du 11 septembre, le Conseil de Sécurité de l'Organisation des Nations Unies a adopté la Résolution 1368 qui établissait une base légale en matière de lutte contre le terrorisme. Peu de temps après, le Conseil de Sécurité adopta la Résolution 1373 qui s'attaquait directement au financement

du terrorisme. Celle-ci exigeait que les 191 États membres, à ce moment, répriment le financement du terrorisme et demandait aux États de criminaliser le support au terrorisme, de geler les fonds, de partager l'information et de fournir de l'assistance technique pour améliorer la coopération (Biersteker et Eckert, 2008). De plus, la Résolution 1373 ordonnait aux États de geler les fonds et autres biens financiers, sans délai, des personnes qui commettent ou tentent de commettre un acte terroriste ou facilitent la commission d'un acte terroriste (de Goede, 2011). En 2001, le Conseil de Sécurité par la Résolution 1333, qui vient compléter la Résolution 1267, demandait de geler les fonds appartenant à Osama Bin Laden et ses associés. Par conséquent, les sanctions ne visaient plus seulement un État, comme avec la Résolution 1267 (Cameron, 2003). Plus tard, le Conseil de Sécurité a donné comme instruction au Comité des Sanctions de maintenir et de mettre à jour la liste des individus et entités désignés comme associés à Osama Bin Laden, incluant Al-Qaïda, laquelle est basée sur des informations fournies par les États (Guild, 2008 ; Cameron, 2003).

Parallèlement à ces dispositions mises en œuvre par l'ONU, différentes organisations se sont également mobilisées à l'échelle mondiale à l'égard de la lutte au terrorisme. Alors que le Groupe d'Action Financière fut créé, de prime abord dans une perspective de lutte contre le blanchiment d'argent, le GAFI « […] a finalement vu son mandat s'étendre jusqu'à la question des fonds terroristes à la suite d'une réunion plénière extraordinaire de ses États-membres qui s'est déroulée à Washington les 29 et 30 octobre 2001 » (Amicelle, 2008, p.132). Par conséquent, le GAFI émit 8 recommandations en octobre 2001, lesquelles étaient majoritairement fondées sur les résolutions de l'ONU (une autre recommandation sera ajoutée plus tard) (Favarel-Garrigues, 2003 ; Foumdjem, 2011). Ainsi, le GAFI recommandait notamment aux « […] États [d']incriminer le financement du terrorisme, [de] geler et confisquer les biens des groupes terroristes et [d']impliquer fortement leurs institutions financières et autres professions concernées afin qu'elles déclarent les transactions suspectées d'être liées au terrorisme » (Chappez, 2003, p.550). Levi (2010) souligne qu'il devenait donc politiquement impossible pour les banques d'omettre d'agir contre le financement du terrorisme.

En parallèle de ces deux organes, d'autres mesures furent prises au niveau international, notamment par la Banque Mondiale et le Fond Monétaire International, comme il a été le cas pour le blanchiment d'argent. Ces acteurs ont reconnu les recommandations émises par le GAFI comme étant les standards devant être appliqués (Biersteker et Eckert, 2008 ; Chappez, 2003). De plus, ils ont notamment développé des plans d'action pour améliorer les efforts de lutte au financement du terrorisme et de lutte au blanchiment d'argent, porté assistance technique à des États et évalué la conformité de certains États (Biersteker et Eckert, 2008).

Ainsi, la collaboration de plusieurs acteurs est requise dans la lutte contre le terrorisme, et ce, tant au niveau national qu'international. D'ailleurs, la liste antiterroriste créée par les Nations Unies est constamment mise à jour à l'aide de renseignements provenant des États. À partir de cette liste, des sanctions ciblées (gel de fonds) sont dirigées vers des individus et des entités. Conséquemment, les sanctions ciblées ne visent plus seulement les gouvernements, mais également les individus (Van Den Herik, 2007 ; Eckert, Biersteker et Tourinho, 2016). Ces sanctions ciblées ont pour but de neutraliser un individu suspecté d'être lié au terrorisme afin d'éviter la commission d'actes terroristes. Il s'agit donc d'une collaboration quant au partage de renseignements, mais également à l'égard de la mise en œuvre de ces sanctions : ce ne sont pas les gouvernements qui mettent en œuvre les sanctions ciblées, mais les banques (Chappez, 2003). Celles-ci jouent donc un rôle décisif dans la lutte au financement du terrorisme.

1.3. La surveillance des flux financiers

1.3.1. Les banques : « des sentinelles de l'argent sale »[4]

La lutte internationale contre le blanchiment d'argent, enclenchée au lendemain du Sommet du G7 en 1989, a imposé une nouvelle fonction aux banques, soit la surveillance des flux financiers (Favarel-Garrigues, Godefroy et Lascoumes, 2009). À la suite du 11 septembre 2001, l'attention portée à la surveillance financière et au renseignement financier s'est intensifiée, venant renforcer par le fait même les mécanismes déjà en place

[4] Favarel-Garrigues, G., Godefroy T. et Lascoumes, P., 2009.

dans la lutte contre le blanchiment d'argent (Amicelle, 2013b). Bien qu'initialement l'attention du GAFI portait sur les banques et les institutions financières, plusieurs acteurs privés se retrouvent désormais en première ligne dans la lutte au financement du terrorisme et au blanchiment d'argent (Svedberg Helgesson et Mörth, 2018 ; de Goede, 2017b). En effet, « Les compagnies d'assurances, les sociétés d'audit et les cabinets d'avocats et de notaires [sont] également soumis aux exigences de vigilance et aux obligations déclaratives » (Amicelle, 2013b). Ces acteurs privés doivent donc « *policer* » leurs clients, au même titre que les banques (Svedberg Helgesson et Mörth, 2018).

Ainsi, la surveillance des flux financiers, effectuée par les banques, permet non seulement de saisir l'argent d'un crime déjà commis, mais permet également d'empêcher la commission de futurs actes (Amicelle, 2013b). D'ailleurs, le renseignement financier, dont la fiabilité est présumée, permettrait de révéler les activités des terroristes, la structure d'un groupe terroriste, leurs logistiques et leurs réseaux (de Goede, 2018 ; Amicelle, 2013b). L'argent sale est donc un problème dont la gestion réside, à la fois, dans le domaine de la sécurité et celui de la finance (Amicelle, 2018). Par conséquent, les banques sont désormais des « sentinelles de la détection et du signalement de l'argent sale » (Favarel-Garrigues, Godefroy et Lascoumes, 2009). De ce fait, elles ont l'obligation légale de connaître leurs clients, de surveiller les comptes et les transactions et éventuellement rapporter les transactions dites suspectes aux autorités responsables, soit l'unité de renseignement financier pour le Canada, le CANAFE ; à défaut de quoi, elles s'exposent à des sanctions pénales et à des risques réputationnels (Amicelle et Iafolla, 2017 ; Amicelle, 2008 ; de Goede, 2017b ; Amicelle, 2018). Afin de satisfaire ces nouvelles obligations, Favarel-Garrigues (2005b) souligne que les banques sont contraintes à réorganiser leurs services : elles doivent procéder à l'embauche de nouvelles personnes, offrir des formations et s'équiper d'outils techniques couteux et de technologies sophistiquées (Favarel-Garrigues, Godefroy et Lascoumes, 2009).

Dans le cadre de leurs obligations, les banques ont dû commencer à surveiller l'identité de leurs clients à l'aide de listes de personnes et d'entités, et ce, depuis 2001 (Favarel-Garrigues, Godefroy et Lascoumes, 2009). Bien qu'il ne s'agisse pas d'une nouvelle pratique, l'utilisation des *blacklists* a pris une forte expansion suite aux évènements du 11

septembre 2001 ; en 2016, il y avait plus de 400 listes dans le monde (Amicelle et Jacobsen, 2016 ; de Goede et Sullivan, 2016). Par conséquent, les banques doivent s'assurer que l'un de leurs clients ne figure pas sur l'une des listes auxquelles elles sont assujetties, soit la liste des Nations Unies (tous les États membres y sont assujettis), la liste du pays où la banque est située, la liste de la banque elle-même et les listes extraterritoriales de différentes juridictions dans la mesure où elle fait affaire avec d'autres pays (de Goede et Sullivan, 2016). Pour ce faire, les banques ont mis en place des instruments automatisés afin de filtrer leurs clients à partir de ces listes (Amicelle, 2019). Dans le cas où un client figure sur l'une de ces listes, la banque doit procéder au gel de fonds. Il s'agit donc de la mise en œuvre de sanctions ciblées, qui visent un individu en particulier et non un pays dans sa totalité, comme les embargos (Van Den Herik, 2007 ; Eckert, Biersteker et Tourinho, 2016). La mise en œuvre de sanctions ciblées par les banques permet d'empêcher un individu étant suspecté d'être lié au terrorisme d'avoir accès à ses ressources financières, voulant ainsi éviter qu'il ne commette des actes terroristes. Il s'agit donc de mesures administratives : n'ayant suffisamment de preuves pour l'accuser criminellement, geler ses fonds permet tout au moins de l'empêcher d'être actif (Guild, 2008). Ainsi, Amicelle et Jacobsen (2016) stipulent que le régime de sanctions ciblées et la régulation de l'argent sale placent les banques en première ligne quant à la sécurisation de la circulation financière.

Selon la logique à l'œuvre, il s'avère donc important pour les banques de connaître leurs clients ; par conséquent, les banques doivent mettre en place le programme *know-your-customer* (KYC) (Ryder, 2012 ; Amicelle et Jacobsen, 2016). Ce programme comprend des procédures pour l'acceptation et l'identification des clients ainsi qu'une surveillance continue des relations d'affaires, particulièrement avec les clients à « haut risque » (Amicelle et Jacobsen, 2016). D'ailleurs, les personnes politiquement exposées[5] sont considérées comme des clients à « haut risque » et sont donc davantage surveillées

[5] « Les personnes politiquement exposées sont des personnes physiques qui occupent ou ont occupé des fonctions publiques importantes, pas nécessairement politiques, liées à un pouvoir de décision significatif. Les personnes considérées comme des personnes connues pour être étroitement associées à un client PPE sont également incluses. » (LexisNexis, s.d.).

puisqu'elles sont plus à risque, notamment à la corruption et au blanchiment d'argent (Levi et Reuter, 2006).

De plus, les banques ont l'obligation de surveiller les transactions et les comptes. À cet égard, la dénonciation des activités suspectes repose sur la surveillance à partir du risque et de l'(a)normalité (Amicelle et Iafolla, 2017). D'une part, calculer le risque posé par les clients permet de déterminer lesquels requièrent une surveillance intensive ; le risque est alors calculé à partir de différents critères tels que la profession, le secteur d'emploi et le pays (Amicelle et Iafolla, 2017). D'autre part, l'(a)normalité permet de déterminer quoi chercher ; les banques peuvent notamment se baser sur des caractéristiques qui ont auparavant mené au blanchiment d'argent ou au financement du terrorisme (Amicelle et Iafolla, 2017 ; Amicelle, 2019). Parmi les indicateurs d'anormalité, il peut s'agir d'un compte réactivé qui démontre des activités significatives ou une transaction excédent 10 000 $, qu'elle soit suspecte ou non (Amicelle et Iafolla, 2017 ; Levi et Reuter, 2006 ; Ryder, 2012 ; Amicelle, 2018). Inversement, il est également possible de déterminer ce qui est « normal » afin de détecter les comportements qui dévient ; il s'agit donc de détecter les comportements inhabituels chez l'utilisateur (Amicelle, 2019 ; Amicelle et Iafolla, 2017). Les logiciels dirigés par des algorithmes visent donc à détecter ces anormalités et à émettre des alertes. Ces logiciels technologiques ont un rôle fort important dans l'analyse des transactions puisque les algorithmes ont la capacité d'analyser de grandes banques de données et d'identifier les anormalités et les patterns déviants (de Goede, 2017b ; Amicelle, 2019). Ces instruments de filtrage permettent également de générer des alertes pour les personnes figurant sur une liste (Amicelle, 2019). Ainsi, les banques doivent effectuer une surveillance nominative, de même qu'une surveillance transactionnelle et comportementale. Or, bien que ces nouveaux outils sophistiqués soient implantés à des fins d'assistance, des difficultés découlent de leur implantation (Favarel-Garrigues, Godefroy et Lascoumes, 2009).

1.3.2. Les critiques associées à la surveillance financière

La surveillance financière dans le cadre de la lutte au blanchiment d'argent et au financement du terrorisme soulève plusieurs débats. D'emblée, bien que les listes

apparaissent comme un moyen technologique contemporain de sécurité et de régulation, de Goede (2011) souligne que l'utilisation des listes noires et des sanctions ciblées, qui gèlent les avoirs d'un compte sur la base d'une suspicion, est l'un des aspects les plus controversés dans la lutte au financement du terrorisme (de Goede et Sullivan, 2016). De prime abord, les listes antiterroristes sont souvent créées sur la base de renseignements humains et de soupçons (Bures, 2012 ; Phillips et Pohl, 2018 ; de Goede, 2011). Par conséquent, il ne s'agit pas nécessairement de terroristes, mais plutôt d'individus suspectés de l'être, basé sur du renseignement ; la décision de placer quelqu'un sur une liste demeure a priori une décision caractérisée par un risque et une incertitude (de Goede et Sullivan, 2016 ; Phillips et Pohl, 2018). D'autre part, les critères quant à l'inclusion sur une liste ne sont pas fixés, et peuvent donc changer. Effectivement, parmi l'abondance de listes, les critères de celles-ci ne sont pas nécessairement rendus publics (de Goede et Sullivan, 2016). Par ailleurs, comme ces listes sont préventives plutôt que punitives, les listes peuvent opérer à l'extérieur du cadre de justice criminelle quant aux standards et protections (de Goede et Sullivan, 2016). Ainsi, plusieurs auteurs s'entendent à l'effet que l'utilisation des listes et des sanctions ciblées va à l'encontre de certains droits et libertés (Amicelle et Favarel-Garrigues, 2009 ; de Goede, 2011 ; Van Den Herik, 2007).

Dans le cadre de l'acquisition de ces listes, les banques peuvent se tourner vers World-Check, une compagnie qui collecte des données et crée des listes pour ensuite en faire la vente, entre autres aux banques (de Goede et Sullivan, 2016). Ces listes sont construites à partir de sources ouvertes, incluant par le fait même différentes listes. Conséquemment, retirer le nom d'un individu s'avère complexe, puisque le retrait d'une liste n'engendre pas systématiquement le retrait de toutes les autres listes (Phillips et Pohl, 2018 ; de Goede et Sullivan, 2016). D'autre part, bien qu'il existe un processus de *delisting*, cet individu peut tout de même constituer un risque pour une banque ; cette dernière peut donc refuser de faire affaire avec lui. Par conséquent, l'individu n'est plus sur une liste, mais aura tout de même des difficultés lors de l'ouverture d'un compte, d'un transfert d'argent, etc. (de Goede et Sullivan, 2016). Par ailleurs, le risque que l'inclusion d'une personne soit erronée demeure, causant malencontreusement des conséquences pour cette personne (Favarel-Garrigues, Godefroy et Lascoumes, 2009 ; Phillips et Pohl, 2018).

Parallèlement, l'utilisation de ces listes engendre la création de faux positifs, c'est-à-dire des liens potentiels (caractéristiques communes, telles que le nom) entre un client et une personne listée, mais qui ne correspondent pas. À cet égard, les banques reçoivent plusieurs alertes, qui sont en réalité des faux positifs, les obligeant à mettre une unité en place afin de gérer ces alertes et ainsi réduire le nombre (Amicelle et Jacobsen, 2015 ; Favarel-Garrigues, Godefroy et Lascoumes, 2009). Ces faux positifs augmentent le risque que d'une part, une sanction soit octroyée à la mauvaise personne, et que d'autre part, des personnes qui figurent sur une liste ne soient pas repérées (Amicelle et Favarel-Garrigues, 2009). De plus, le nombre de listes et le nombre de personnes listées ne cessent d'accroître, augmentant par le fait même le nombre de faux positifs (Burges, 2012).

De même, l'utilisation de nouvelles technologies et d'algorithmes à des fins de détection au sein de grandes bases de données, occasionnent de nombreux faux positifs (Amicelle, 2019). Par conséquent, il s'agit d'un défi de taille pour les banques de devoir trier ces alertes générées par des logiciels, ce qui engendre des coûts importants (Amicelle, 2019). Ainsi, malgré le fait que ces outils technologiques soient utilisés dans une perspective d'amélioration des pratiques en matière de surveillance financière, ces technologies sophistiquées ne sont pas la solution à toutes les difficultés et incertitudes rencontrées par les banques (Favarel-Garrigues, Godefroy et Lascoumes, 2009). De surcroît, l'implantation de ces technologies sophistiquées au sein des banques engendre des coûts exorbitants pour celles-ci (Favarel-Garrigues, Godefroy et Lascoumes, 2009 ; Roberge, 2004). De plus, en raison de l'évolution fulgurante des technologies, celles-ci nécessitent continuellement des mises à jour (Amicelle, 2019).

Par ailleurs, la surveillance comportementale a également été critiquée dans le cadre de la lutte au blanchiment d'argent et au financement du terrorisme. Effectivement, le présupposé qu'il est possible de distinguer le comportement financier criminel du comportement financier « normal » suscite de nombreux débats, principalement quant au financement du terrorisme (Amicelle et Iafolla, 2017). En effet, les criminels et les terroristes vont volontairement masquer leurs intentions et tenter d'avoir un comportement « normal » afin d'être difficilement distinguables des autres clients bancaires (Amicelle et Iafolla, 2017). De plus, lors de l'identification de comportements « anormaux » par les

banques, les soupçons à cet égard doivent être suffisamment importants pour que des renseignements confidentiels soient transmis à la police afin d'éviter de brimer le droit à la vie privée (Roberge, 2004). Enfin, les analyses comportementales peuvent mener à de mauvaises détections d'opérations, lesquelles sont seulement, légèrement, inhabituelles, soit un montant ou un destinataire inhabituel chez un client (Favarel-Garrigues, Godefroy et Lascoumes, 2009).

Bien que les mesures visant à contrer le financement du terrorisme sont considérées comme un fondement dans la lutte au terrorisme, certains auteurs ne sont pas disposés à dire de même (Bures, 2012). Effectivement, Eckert (2008) pense qu'il est irréaliste de croire que ces mesures pour lutter le financement du terrorisme peuvent effectivement contrer ce phénomène ou éliminer complètement les sources d'argent ; tout au plus, ces mesures rendent l'utilisation du système financier formel plus difficile pour les terroristes. Ainsi, les terroristes obtiennent encore du financement, mais par différents moyens informels. Parallèlement, selon Levi (2010), puisqu'on ne peut savoir le nombre d'attentats évités à l'aide des mesures utilisées pour contrer le financement du terrorisme, il est possible que le terrorisme soit tout simplement restructuré plutôt qu'éradiqué : en réduisant leur capacité financière, les terroristes ont moins de moyens pour effectuer des attentats spectaculaires, mais demeurent actifs. Enfin, Steinbock (2006) souligne que bien souvent, ceux qui commettent des attentats terroristes, n'étaient pas connus des services policiers, donc n'étaient pas sur une liste antiterroriste de prime abord. À l'inverse, Phillips et Pohl (2018) mentionnent que le fait d'être sur l'une de ces listes n'empêche pas avec certitude la commission d'actes terroristes par ces individus. Effectivement, des individus, qui étaient a priori sur une liste, ont tout de même commis des actes terroristes : l'un des deux terroristes de l'attentat du marathon de Boston et l'auteur d'un incident terroriste à Melbourne en 2017. Conséquemment, bien qu'il y ait des listes et que des alertes soient censées être émises lors de la présence de l'un de ces individus dans un lieu surveillé, tel qu'une banque et un aéroport, ou lors de la réalisation d'une transaction financière, il est possible que le nom ne soit pas détecté (Phillips et Pohl, 2018).

Ainsi, différents outils technologiques sont utilisés afin d'aider les banques dans le cadre de leurs obligations à l'égard de la lutte au financement du terrorisme et du blanchiment

d'argent. D'ailleurs, plusieurs écrits critiquent ces outils, mais très peu traitent de la façon dont ces outils technologiques sont réellement mobilisés par les banques. Dans cette perspective, peu de littérature porte sur l'implantation et les impacts des technologies dans la lutte à l'argent sale. Bien qu'il y ait des écrits sur les nouvelles technologies, très peu abordent les technologies au sein des banques ; le *Big Data*, les enjeux en matière de surveillance et les technologies financières sont peu couverts par la littérature.

2. Les nouvelles technologies de surveillance

2.1. Les pratiques en matière de surveillance

2.1.1. L'émergence du Big Data : la solution aux problèmes de sécurité

Les technologies ont pris une place indéniable au sein de la société et évoluent à une vitesse fulgurante. Par conséquent, chaque domaine de la société doit s'ajuster à l'avènement de nouvelles technologies et faire progresser leurs pratiques en ce sens. Ainsi, les pratiques en matière de surveillance changent et sont reconfigurées de différentes façons, et ce, à l'ère de ces nouvelles technologies (Lyon, 2014). L'un de ces changements se situe au niveau de la collecte et de l'utilisation des données à des fins de surveillance, le *Big Data* (Lyon, 2014). Les révélations d'Edward Snowden en 2013 ont marqué un tournant décisif dans l'histoire de la surveillance, soulevant par le fait même la question du *Big Data* (Pasquale, 2016 ; Lyon, 2014). Ces révélations portaient sur la « coopération consciente » entre de grandes compagnies des hautes technologies et des communications, telles que Facebook, Google et Apple, et l'État, plus précisément la National Security Agency (NSA) aux États-Unis (Pasquale, 2016 ; Dijck, 2014 ; Lyon, 2014). Les pratiques de surveillance révélées par Snowden ont donc démontré que les gouvernements, notamment américain et canadien, surveillaient la population, et ont aussi dévoilé la façon dont cette surveillance était orchestrée (Lyon, 2014). Des métadonnées[6] étaient recueillies à l'insu des utilisateurs, une collecte qui avait été autorisée aux États-Unis suite au 11 septembre 2001, et ce, dans une perspective de lutte au terrorisme (Lyon, 2014). Par conséquent, l'utilisation des données à des fins de sécurité est redevenue un problème politique (Bauman et al., 2015 ; Aradau

[6] Il s'agit de données sur les données, tel que l'adresse IP, l'identité de la personne contactée, la durée de l'appel, etc. (Lyon, 2014).

et Blanke, 2015). Bien qu'il ne s'agisse pas de nouveaux débats quant à la sécurité des données, ceux-ci ont été ravivés par les révélations de Snowden et l'émergence du *Big Data*. De nouveaux débats furent également suscités quant aux pratiques numériques et aux dispositifs de *Big Data* utilisés à des fins de sécurité (Aradau et Blanke, 2015).

Ces pratiques de *Big Data* sont utilisées par les gouvernements à des fins de sécurité certes, mais elles sont aussi utilisées par les entreprises privées qui recueillent des données, notamment à des fins de marketing et de publicités (Rouvroy et Berns, 2013). Il s'agit donc de données en quantité massive, lesquelles sont collectées et conservées de façon automatisée et non classée (Rouvroy et Berns, 2013 ; Amicelle, 2019). Ces données sont souvent générées de façon continue : les appareils numériques enregistrent l'historique de leur utilisation (cellulaire), les transactions bancaires, etc. (Kitchin, 2014a). Elles peuvent donc être de différentes origines et donc provenir de différentes sources et en différents formats (Cardon, 2015 ; Amicelle, 2019). Il devient donc aujourd'hui de plus en plus difficile d'éviter de laisser des traces des actions quotidiennes en raison des technologies numériques. En effet, au-delà des transactions bancaires, la simple présence d'un individu dans un magasin est enregistrée par des caméras de surveillance, ou encore la disponibilité de l'adresse IP d'un ordinateur, bien que l'individu soit anonyme. Par conséquent, le volume et la variété des données générées sur tous les aspects de la vie ne cessent d'augmenter (Kitchin, 2014b). On peut dès lors en savoir beaucoup sur un individu à partir des données recueillies : son travail, ses voyages, ses communications, ses intérêts, etc. Jamais auparavant autant de données n'étaient disponibles sur les individus et souvent, ceux-ci ont peu de contrôle sur la façon dont leurs données seront utilisées (Kitchin, 2014b).

Par ailleurs, Lyon (2014) souligne que les pratiques de *Big Data* fonctionnent en sens inverse du renseignement policier et du renseignement de sécurité conventionnels : plutôt que cibler un suspect et chercher des données sur celui-ci, des données de masse sont recueillies provenant de différentes sources, avant même de déterminer leur potentielle utilité. Ces données seront éventuellement analysées par des algorithmes à l'égard d'actions passées, mais aussi afin de prédire et ainsi intervenir avant la commission de futurs actes. Ces données sont donc conservées dans un *datawarehouses* avant d'être

potentiellement utilisées (Rouvroy et Berns, 2013). Par conséquent, pour les professionnels de la sécurité, l'analyse prédictive avec le *Big Data* maintient la promesse de sécuriser le futur en anticipant la « prochaine attaque terroriste » et appréhendant les criminels potentiels avant qu'ils agissent (Aradau et Blanke, 2017). Effectivement, l'émergence du *Big Data* a été jointe à la promesse de trouver « *the needle in the haystack* », considérant désormais l'ancienne approche insuffisante : *Connecting the dots* (Aradau et Blanke, 2017). Ainsi, pour les professionnels en sécurité, le *Big Data* apparaît comme étant la solution aux problèmes de sécurité contemporains, promettant de révolutionner les pratiques en sécurité, en contreterrorisme, en protection des frontières, etc. : le *Big Data* et l'analyse prédictive dévoilent des patterns inattendus et repèrent de potentielles aiguilles (*needles*) suspectes (Chan et Bennett Moses, 2017 ; Aradau et Blanke, 2015 ; Aradau et Blanke, 2017).

Les promoteurs du *Big Data* ont promis de révolutionner les capacités digitales et les pratiques de gouvernance (Aradau et Blanke, 2017). Ainsi, les pratiques de *Big Data* ont été adoptées et se sont répandues rapidement, produisant des changements dans les organisations du secteur public et privé (Lyon, 2014). La collection de données de masse permet donc de révéler des patterns par l'utilisation d'algorithmes qui effectuent l'analyse ; le traitement de données de masses se situe au-delà de la capacité humaine, nécessitant l'utilisation d'outils très performants (Lyon, 2014 ; Chan et Bennett Moses, 2017).

2.1.2. L'utilisation des algorithmes dans le domaine de la sécurité

À l'ère du numérique, les algorithmes sont dès lors utilisés dans la vie de tous les jours : ils organisent le fil d'actualité sur les réseaux sociaux, suggèrent ce qui pourrait intéresser l'utilisateur (Netflix et Amazaon), etc. (Thomas, Nafus et Sherman, 2018 ; Cardon, 2015). Ainsi, Cardon (2015) souligne que très peu d'actions quotidiennes, d'achats, de déplacements ne sont pas dirigés par une « infrastructure de calculs ». Les algorithmes sont donc utilisés dans plusieurs domaines tels que la finance, le transport et la santé. (Cardon, 2015). De même, ils sont utilisés à des fins d'analyse de *Big Data* ; « [un algorithme] opère un ensemble de calculs à partir de gigantesques masses de données (*Big Data*) » (Cardon, 2015, p.7). Le défi est de créer des façons de lier ces données ensemble, lesquelles peuvent

varier de par leurs natures (par exemple métadonnées et données standards) et varier quant à leurs finalités initiales au moment de la collecte (Lyon, 2014 ; Kitchin, 2014b). Il s'agit ainsi d'une tâche complexe à laquelle les algorithmes peuvent porter assistance, notamment par la recherche et le regroupement des données : *connecting the dots* (Kitchin, 2014b ; Amoore, 2009). À cet effet, les enquêtes sur les évènements du 11 septembre 2001 ont révélé qu'il y avait suffisamment d'informations dans les bases de données permettant la prévention de ces évènements : si les données avaient été connectées ensemble, les évènements auraient pu être évités (Amoore, 2009). Conséquemment, l'accent était mis sur la nécessité de connecter les points (les informations reliées au terrorisme) plus efficacement (Amoore, 2009). Cette approche permet également de détecter des patterns parmi les données qui pointeraient vers une personne ou un groupe suspect dont les associations et communications mèneraient à une personne d'intérêt (Lyon, 2014). Les algorithmes rendent donc possible la transformation de probables associations entre des personnes ou des objets en « *actionnable security decisions* » (Amoore, 2009). Bien que cette approche soit une possibilité, les algorithmes sont désormais plutôt utilisés dans le domaine de la sécurité dans une perspective de « *finding the needle in the haystack* », tel que mentionné précédemment (Aradau et Blanke, 2017).

Ainsi, les algorithmes sont déployés à plusieurs finalités dans le domaine de la sécurité. Au-delà de ce qui a été mentionné précédemment, les algorithmes, joints à des associations, peuvent calculer les menaces liées à la sécurité d'un aéroport : Est-ce que l'individu a payé en argent comptant ? ; Est-ce qu'il est un voyageur fréquent ? ; etc. À partir de ces informations, un calcul basé sur ce qui est la norme et ce qui dévie de la norme engendrera une alerte ou non (Amoore, 2009). Ces calculs algorithmiques permis par les technologies sont de plus en plus présents dans une perspective de Guerre contre le terrorisme (Amoore, 2009). D'autant plus, les algorithmes joints à des caméras de surveillance sont en mesure d'identifier des visages et permettent aussi l'identification de véhicules à partir des plaques d'immatriculation (Dupont, 2004). De surcroît, au sein des pratiques policières, la police prédictive se base notamment sur la supposition qu'il est possible d'utiliser la technologie pour prédire un crime avant qu'il arrive : ces logiciels utilisent des algorithmes complexes (Bennett Moses et Chan, 2018). D'autre part, la lutte au blanchiment d'argent et au

financement du terrorisme requiert des instruments algorithmiques afin de surveiller les flux financiers et ainsi détecter les activités suspectes (Amicelle, 2019). Parallèlement, les algorithmes sont aussi employés dans le cadre de la gestion des listes antiterroristes : lors du gel des avoirs d'un individu par les banques et à des fins de surveillance (Amoore, 2009 ; Phillips et Pohl, 2018). À cet égard, certains individus placés sur ces listes vont faire l'objet d'une surveillance constante. De ce fait, des données sont recueillies sur ces individus, dont leurs communications et leurs activités sur internet. Des algorithmes sont dès lors utilisés afin d'identifier certains patterns ; ceux-ci vont donc émettre une alerte lorsque l'activité internet de l'un de ces individus révèle des informations éloquentes (Phillips et Pohl, 2018).

Toutefois, il s'agit d'une tâche difficile à laquelle sont confrontés les ordinateurs et algorithmes, occasionnant des erreurs et des omissions de détection (Phillips et Pohl, 2018). De plus, à l'heure actuelle, la prochaine attaque terroriste demeure imprévisible et les évènements futurs diffèrent déjà des évènements précédents (Aradau, 2015). De surcroît, les algorithmes, utilisés avec les caméras de surveillance, ne détectent pas nécessairement tous les visages en raison de la qualité des caméras, de l'angle, des expressions du visage, etc. (Dupont, 2004). Ainsi, bien que les nouvelles technologies apparaissent comme une solution à l'ère du numérique dans plusieurs champs, dont celui de la sécurité, il n'en demeure pas moins que des problèmes et des préoccupations découlent de leur utilisation. « Les technologies de sécurité sont [alors] le résultat de controverses, de rapports de force et donc de débats entre une myriade d'acteurs de conceptions, d'intérêts, de buts et de valeurs » (Amicelle, 2019).

2.1.3. Préoccupations légales et techniques

La surveillance fait désormais partie de la vie quotidienne où la société est plus sujette à une scrutation, et ce, par différents modes de surveillance (Bauman et al., 2015 ; Kitchin, 2014b). Effectivement, de plus de plus de technologies sont utilisées à des fins de surveillance (scanner corporel, biométrie, caméras de surveillance toujours plus performantes, etc.), lesquelles peuvent être de plus en plus intrusives et souvent justifiées par la Guerre au terrorisme ; ce qui rappelle d'ailleurs la collecte de métadonnées par le

gouvernement américain (Ceyhan, 2008). Or, Lyon (2014) souligne que la question du *Big Data* jointe aux révélations de Snowden ont suscité un intérêt public quant à la surveillance dans plusieurs pays. Ainsi, la surveillance est aujourd'hui un sujet controversé : pour certains la surveillance n'est pas considérée problématique, sous prétexte qu'une personne qui n'a rien à se reprocher devrait accepter de partager ses données, alors que pour d'autres il s'agit d'une violation significative à leur droit à la vie privée (Pasquale, 2016 ; Kitchin, 2014b). Ceci dit, plusieurs auteurs s'entendent que les pratiques de *Big Data* vont effectivement à l'encontre de la vie privée et donc de la protection des droits et libertés (Aradau et Blanke, 2015 ; Lyon, 2014 ; Pasquale, 2016 ; Bauman et al., 2015). Le droit à la vie privée est fondamental pour une multitude d'individus, il s'agit d'un droit significatif allant de soi. D'autant plus, la vie privée est considérée comme un droit de l'homme et est protégée par des lois nationales et supranationales (Kitchin, 2014b). Bauman et al. (2015) soulignent qu'il s'agit d'ailleurs d'un devoir de l'État de protéger les données personnelles.

Comme il a été mentionné, les professionnels de la sécurité mettent de l'avant *finding the needle in the haystack* (Aradau et Blanke, 2017). Cependant, peu importe la quantité de données disponibles, ce n'est jamais complet et le volume peut submerger les signaux critiques dans un brouillard de corrélations possibles (Chan et Bennett Moses, 2017). D'autre part, Lyon (2014) souligne qu'il y a une forte probabilité que cette approche engendre des faux positifs. Parallèlement, certains dispositifs utilisés en renseignement font des erreurs remarquables, ignorent de réelles menaces ou inversement ciblent les mauvaises personnes (Pasquale, 2016). En fait, il s'agit d'un défi de taille à l'égard de l'analyse du *Big Data* où une abondance et une variété de données sont disponibles (Kitchin, 2014a). Cardon (2015) souligne également qu'un des enjeux du *Big Data* est de donner une signification à ces « données brutes » ; ces données sont souvent générées sans avoir de finalités particulières (Kitchin, 2014b). De plus, le *Big Data* propose une multitude de données structurées et non structurées, une exhaustivité des données et présente donc des incertitudes (Kitchin, 2014b).

De surcroît, les pratiques reliées au *Big Data* encouragent l'utilisation de décisions automatiques, notamment par des algorithmes, réduisant par le fait même le rôle de la discrétion (Lyon, 2014). Des décisions importantes sont prises de façon automatisée

pouvant entrainer des conséquences significatives : le programme *data matching* « *No Fly* », du gouvernement fédéral américain, identifie certains individus comme de potentiels terroristes, les interdisant de voyager, et entrainant par conséquent des limitations à leurs droits et libertés (Lyon, 2014). Parallèlement, les algorithmes peuvent fonctionner de façon biaisée. En effet, des modes de gouvernance anticipatoire soulèvent des problèmes éthiques puisque leur attention vise certains groupes et certains endroits. D'autant plus, ils cherchent à policer des comportements qui peuvent ne jamais survenir et par ce processus, restructurent la façon dont les gens devraient agir par l'autodiscipline (Kitchin, 2014b). L'analyse prédictive intensifie donc souvent les préjugés et la discrimination (Kitchin, 2014b).

Les pratiques de *Big Data* en matière de surveillance sont davantage axées sur le futur plutôt que sur le passé ou le présent. Cette anticipation place donc plus de poids sur la surveillance dans le but de gérer les conséquences plutôt que chercher à comprendre les causes des problèmes sociaux comme le crime et le désordre (Lyon, 2014).

> « Les nouvelles technologies d'identification et de surveillance offrent des méthodes sophistiquées pour faire face aux risques. Mais, cette offre crée une demande sans fin, incitant les acteurs scientifiques et économiques à chercher toujours une technologie meilleure que la précédente pour circonscrire les incertitudes et de nouveau confronter, en innovant, les risques connus. Cette quête de meilleure technologie est devenue l'un des enjeux politiques majeurs de notre temps, car elle participe à la prétention de l'État à maîtriser l'incertitude et contrôler le futur. » (Ceyhan, 2006, p.7).

Ainsi, les pratiques en matière de *Big Data* et l'utilisation des algorithmes soulèvent plusieurs enjeux. Or, les recherches sur les impacts de la technologie sur les organisations policières remontent bien avant l'arrivée des recherches sur le *Big Data* et les algorithmes. À cet égard, Chan et Bennett Moses (2017) soulignent qu'il y a un manque de recherches empiriques sur les impacts des changements technologiques sur les pratiques de sécurité ; les écrits actuels concernent principalement le *policing* et l'application de la loi.

2.2. La technologie au sein des organisations de *policing* : les impacts

2.2.1. L'implantation de nouvelles technologies

L'utilisation des technologies de l'information est devenue partie intégrante de la vie de tous les jours au courant du 21e siècle pour une multitude d'individus certes, mais également pour la majorité des organisations (Chan, 2001). À cet égard, selon Rogers (2003), la taille d'une organisation est positivement liée à son caractère innovant : plus une organisation est de taille importante, plus elle aura tendance à innover. Or, plusieurs raisons peuvent pousser une entreprise à innover et intégrer de nouvelles technologies dans leurs méthodes de travail (Rogers, 2003). Chan (2001) souligne qu'au sein des organisations policières, la motivation d'intégrer la technologie dans leurs pratiques provenait d'un désir d'améliorer l'efficacité et l'efficience, de satisfaire aux demandes des agences externes pour l'information et pour rencontrer les exigences des nouvelles formes de gestion et responsabilité de la police (Ratcliffe, 2016). D'autre part, Dupont (2004) mentionne que parmi les institutions étatiques, l'organisation policière est l'une qui a été le plus touchée par le développement des sciences et des technologies. En effet, alors que toutes les organisations font l'utilisation de technologies, Ericson et Haggerty (1997) précisent que la police a été l'un des chefs de file en matière d'adaptation et de développement technologiques. Par conséquent, les écrits recensés portent essentiellement, voire uniquement sur l'implantation de technologies au sein des organisations policières, lesquelles font face à des difficultés similaires que celles rencontrées par les autres organisations. Or, quelques écrits sur les organisations non policières seront également joints à cette recension.

L'ère des nouvelles technologies incite les organisations policières à obtenir des dispositifs de plus en plus perfectionnés (Dupont, 2004). De prime abord, les organisations policières font l'utilisation de technologies sophistiquées quotidiennement dans le cadre de leur travail et cherchent constamment à améliorer leurs solutions informatiques (Ericson et Haggerty, 1997). Cette aspiration à innover technologiquement amène les grandes organisations policières à se doter d'effectifs à plein temps, afin de trouver de nouvelles solutions informatiques permettant de s'adapter continuellement aux changements

(Ericson et Haggerty, 1997). D'autre part, différentes raisons peuvent motiver les organisations policières à se procurer des technologies informatiques ; elles y voient le moyen de résoudre les difficultés auxquelles elles sont confrontées dans leurs tâches quotidiennes, dont la charge administrative. Effectivement, certaines technologies informatiques furent implantées afin d'une part, réduire la charge administrative par l'utilisation d'appareils plus performants et rapides et d'autre part, réduire l'utilisation du papier. Enfin, ces technologies offrent aussi un sentiment de sécurité organisationnel et une source de légitimation organisationnelle où elles symbolisent la compétence d'une organisation (Ericson et Haggerty, 1997). À cet effet, l'importance accordée aux innovations au sein d'une organisation s'est intensifiée, notamment en raison de la propagation des nouvelles technologies de communication introduites dans les organisations (Rogers, 2003).

Bien que plusieurs raisons motivent ces organisations à faire l'acquisition de nouvelles technologies, lorsqu'une organisation décide officiellement d'adopter ces technologies, l'implantation ne suit pas toujours directement (Rogers, 2003). En effet, Tanner et Meyer (2015) soulèvent que lors du processus d'introduction, chaque dispositif de sécurité doit passer un test d'utilité et démontrer son aptitude à opérer en concordance avec le travail déjà en place au sein de l'organisation policière. Ceci dit, l'introduction de nouvelles technologies n'a pas toujours l'effet escompté, bien qu'elles soient introduites dans un but précis (Chan, 2001). Effectivement, plusieurs problèmes peuvent découler suite à l'implantation d'innovations au sein d'une institution (Rogers, 2003). D'une part, cette implantation peut représenter un changement majeur au niveau des comportements humains et dès lors requérir une période d'apprentissage pour les membres du personnel (Rogers, 2003). D'autre part, les supérieurs peuvent avoir des attentes irréalistes vis-à-vis la capacité des nouvelles technologies : Ratcliffe (2016) souligne que des commandants s'attendent à ce que le système « crache » la réponse. Parallèlement, il peut y avoir une divergence quant aux finalités de l'implantation de technologies entre les utilisateurs et les architectes. Cette incongruence peut donc poser problème lors de l'implantation (Chan et Bennett Moses, 2017). Ainsi, selon Rogers (2003), l'implantation de plusieurs innovations

fut peu éloquente, d'où l'intérêt de mieux comprendre comment introduire de façon efficace les technologies informatiques.

2.2.2. Les transformations au sein des pratiques

L'introduction de nouvelles technologies au sein d'une organisation apporte des changements au niveau des pratiques, auxquels les membres du personnel doivent s'adapter. Bien qu'il puisse s'agir de changements importants, ces nouvelles technologies sont souvent implantées dans le but d'ultérieurement améliorer les performances de l'institution (Sasidharan, 2015). En effet, la numérisation des dossiers policiers a permis aux policiers d'être plus efficients dans leurs tâches et leur a donné la possibilité de procéder à des analyses qu'il n'était possible d'effectuer auparavant (par exemple l'analyse des empreintes digitales) (Ratcliffe, 2016). D'autant plus, la numérisation fut implantée afin de remplacer les rapports écrits à la main dans une perspective d'efficacité (Tanner et Meyer, 2015 ; Éricson et Haggerty, 1997). De plus, la numérisation des équipements dans les voitures policières permet d'être constamment connecté avec les bases de données, apportant des changements significatifs au niveau de l'équipement certes, mais du travail policier aussi (Tanner et Meyer, 2015 ; Dupont, 2004 ; Byrne et Marx, 2011). De surcroît, l'implantation de technologies au sein des organisations policières a facilité l'analyse des appels téléphoniques, a permis de suivre les transactions financières électroniques, de cartographier des réseaux sociaux, de lire les plaques d'immatriculation, etc. (Ratcliffe, 2016 ; Byrne et Marx, 2011). Ces innovations technologiques furent donc développées et implantées afin d'améliorer la performance policière, mais également afin de prévenir le crime (Byrne et Marx, 2011). Enfin, ces technologies peuvent aussi être implantées à des fins de sécurité pour les policiers : le *taser*, la voiture de police, etc. (Byrne et Marx, 2011).

Bien que ces technologies soient implantées dans une perspective d'efficacité, l'implantation ne concorde pas nécessairement avec les attentes initiales, comme précédemment mentionné (Chan, 2001). Effectivement, il est possible que les technologies produisent des effets inattendus et non désirés (Amicelle, 2019 ; Chan et Bennet Moses, 2017). D'ailleurs, Chan (2001) a observé que les policiers passent plus de temps à utiliser la technologie au travail qu'auparavant. De plus, alors que la numérisation avait entre

autres pour objectif de réduire la charge administrative et réduire le papier, Ratcliffe (2016) souligne que certains systèmes informatiques sont utilisés conjointement avec les formats papier plutôt que comme remplacement, à des fins de sauvegarde. Par conséquent, dans certains cas, le policier doit compléter des informations à l'ordinateur ainsi que compléter une version papier (Ratcliffe, 2016 ; Ericson et Haggerty, 1997). Parallèlement, l'une des finalités des ordinateurs dans les voitures était d'éviter que les policiers retournent au poste de police pour remplir des documents, permettant ainsi de passer plus de temps dans la rue. Toutefois, plusieurs préfèrent utiliser les ordinateurs de bureau et passent davantage de temps au bureau, créant ironiquement une distance du public (Ericson et Haggerty, 1997). De même, Dupont (2004) souligne que ces technologies implantées dans les organisations policières, notamment les voitures, créent une barrière entre les policiers et les citoyens. Or, bien que certaines innovations technologiques introduites dans le travail policier règlent certains problèmes, d'autres en découlent (Ericson et Haggerty, 1997). En effet, la plupart des innovations causent des conséquences désirables et non désirables (Rogers, 2003). Pour contrer certaines de ces conséquences, une innovation peut être modifiée afin de s'adapter à l'organisation ou la structure de l'organisation peut être changée pour s'adapter à l'innovation, notamment par la création d'une nouvelle unité (Rogers, 2003).

2.2.3. Les défis d'implantation auxquels les organisations sont confrontées

L'implantation de technologies au sein des organisations peut être accueillie de différentes façons par le personnel ; une implantation touche plusieurs individus et engendre donc des opinions en faveur et en défaveur de la nouvelle idée (Roger, 2003). Effectivement, certains voient la technologie comme un outil permettant de prendre en charge les tâches moins intéressantes du quotidien, alors que d'autres considèrent plutôt que la technologie prendra ultérieurement leur place et leur travail (Eason, 1988). Par conséquent, il est possible qu'il y ait la présence d'une résistance de la part des employés face à l'implantation de nouveaux systèmes (Chan, 2001 ; Éricson et Haggerty, 1997 ; Rogers, 2003). En effet, Chan (2001) rapporte que des policiers avaient résisté à certains aspects des technologies de l'information, notamment par le refus de participer. Les policiers percevaient ces technologies comme un outil de surveillance ou considéraient que le système était difficile et fastidieux (Chan, 2001). Des changements radicaux au sein d'une institution peuvent

donc générer de l'hostilité et de la rancœur (Sasidharan, 2015). D'autant plus, certaines innovations créent un haut degré d'incertitude dans une organisation, un état inconfortable qui peut amener la résistance à la technologie (Rogers, 2003). D'autre part, dans le cas d'une organisation policière, la culture policière[7] est endurcie, laquelle résiste et dévie les incursions technologiques (Ericson et Haggerty, 1997). En revanche, il est également intéressant de noter que Rogers (2003) souligne que la structure organisationnelle peut résister à l'implantation d'innovations, et ce, dans le cadre d'une organisation non policière. Dupont (2004) souligne aussi qu'il peut être difficile d'imposer l'utilisation de nouvelles technologies aux policiers, plus particulièrement si elles touchent au pouvoir discrétionnaire des policiers ; ils ont l'impression d'être disciplinés, car tout est documenté (Ericson et Haggerty, 1997). Par ailleurs, certains y voient plutôt une dépendance à la technologie et l'impossibilité de postérieurement travailler sans le dispositif : si les outils technologiques sont en panne ou interrompus temporairement, une grande partie du travail administratif serait paralysé (Tanner et Meyer, 2015). D'autre part, comme l'ordinateur dans la voiture est petit, plusieurs préfèrent retourner au poste de police pour compléter le rapport sur un ordinateur de plus grande taille. Par conséquent, cette situation réduit la présence de policier dans les rues en raison de ces dispositifs (Tanner et Meyer, 2015).

Parallèlement, les nouveaux dispositifs technologiques demandent beaucoup de temps et d'énergie, afin d'apprendre à les utiliser adéquatement (Tanner et Meyer, 2015). Certains policiers ne sont pas en mesure de faire la transition et ne sont pas complètement en contrôle des nouveaux dispositifs ; même après plusieurs années, certains ont toujours des difficultés à utiliser les nouveaux systèmes. Certains ne sont pas capables de mémoriser les procédures pour utiliser le système à son plein potentiel (Tanner et Meyer, 2015). Ericson et Haggerty (1997) rapportent qu'un policier trouvait que les nouveaux systèmes informatiques étaient trop difficiles à utiliser et cela lui prenait plus de temps que remplir à la main et refusait ainsi de l'utiliser.

[7] « Police culture (or subculture) refers to the mix of informal prejudices, values, attitudes and working practices commonly found among the lower ranks of the police that influences the exercise of discretion. It also refers to the police's solidarity, which may tolerate corruption and resist reform. » (Waddington, 2008, p.203).

Ceci dit, bien que certains soient critiques quant à l'implantation de nouveaux dispositifs de sécurité, certains policiers sont plutôt optimistes : ils croient que la technologie est une façon de simplifier leur travail et d'augmenter l'efficience policière (Tanner et Meyer, 2015). D'ailleurs, Ratcliffe, (2016) rapporte que les policiers sont plus susceptibles d'utiliser les technologies pour les assister dans leurs activités traditionnelles (localiser une personne d'intérêt), que les utiliser à des fins de tâches proactives (résolution préventive de problèmes). Parallèlement, l'utilisation du *Big Data* par les organisations policières est plus aisément agréée afin de faciliter leur travail que de changer la nature de celui-ci (Chan et Bennett Moses, 2017). Conséquemment, la technologie est davantage acceptée si elle est implantée à des fins d'amélioration des tâches traditionnelles, plutôt qu'à des fins de définition de nouvelles tâches (Ratcliffe, 2016).

Bien que l'introduction d'innovations au sein d'une organisation vise entre autres l'amélioration des pratiques, certaines répercussions peuvent en résulter. Effectivement, des problèmes peuvent découler de l'implantation de technologies, des problèmes qui n'étaient pas connus au moment de l'introduction par l'organisation, voire par l'inventeur (Dupont, 2004). D'autant plus, ces problèmes ou défauts reliés aux technologies ne seront pas nécessairement réglés immédiatement lors de la détection (Dupont, 2004). De plus, les concepteurs des technologies ne peuvent prévoir tous les effets de celles-ci, des effets qui n'auront lieu qu'au moment où les utilisateurs en feront l'utilisation (Amicelle, 2019). Parallèlement, l'implantation de technologies plus efficientes peut, dans certains cas, produire plus de données qu'auparavant. Par conséquent, des experts sont nécessaires et parfois d'autres technologies afin de gérer ces données (Rogers, 2003). Enfin, bien que des outils de plus en plus performants soient utilisés par les organisations policières, du moins celles qui possèdent les moyens, Dupont (2004) et Byrne et Marx (2011) rapportent que leurs performances ne sont pas améliorées.

D'autre part, la technologie évolue rapidement, de telle sorte que des policiers critiquent l'organisation policière de ne pas être en mesure de changer de façon expéditive ; ils nomment entre autres des problèmes avec l'obsolescence et l'irrégularité de remplacement (Tanner et Meyer, 2015). Les technologies nécessitent aussi des mises à jour

continuellement (Tanner et Meyer, 2015). Dû à cette vitesse d'évolution, la dernière innovation devient rapidement obsolète (Dupont, 2004 ; Ericson et Haggerty, 1997).

> « Les ambivalences du progrès technique sont masquées par les sophismes de la nouveauté et de la plausibilité apparente. Le premier assume que tout ce qui est nouveau est par définition meilleur que ce qui est plus ancien, et connaît un succès indiscutable dans nos sociétés où l'innovation technique connaît des cycles de plus en plus courts. […] [L]e sophisme de la plausibilité apparente, qui justifie l'adoption inconditionnelle des nouvelles technologies par une appréciation de bon sens quant à leur efficacité, fait le sacrifice d'évaluations rigoureuses et de débats rationnels au profit de la solution miracle, qui tire son infaillibilité de son degré de technologie. » (Dupont, 2004, p.117).

CHAPITRE 2 – PROBLÉMATIQUE

Au courant des dernières décennies, le blanchiment d'argent devint un enjeu international, d'où la nécessité d'une mobilisation à l'échelle mondiale. Parallèlement, les attaques terroristes du 11 septembre 2001 ont intensifié l'attention portée au terrorisme internationalement ; c'est ainsi qu'une lutte contre le blanchiment d'argent et le financement du terrorisme, conjointement, s'est développée, laquelle fut l'objet de nombreuses recherches scientifiques. Selon certains acteurs du milieu, éliminer les sources d'argent des terroristes permettrait d'éradiquer ce phénomène, d'où l'importance du rôle des banques dans la lutte au terrorisme. La surveillance des flux financiers permettrait d'intervenir à la suite d'un crime (blanchiment d'argent), mais aussi avant la commission d'un acte criminel (financement du terrorisme). Les banques se sont donc retrouvées avec de nouvelles obligations, étant considérées comme des « sentinelles de l'argent sale », jouant un rôle en première ligne dans la lutte au financement du terrorisme et du blanchiment d'argent. Plusieurs auteurs se sont d'ailleurs attardés à ces nouvelles obligations qui leur sont imposées. Afin de les assister dans ces nouvelles obligations, les banques se sont dotées d'outils informatiques, lesquels sont de plus en plus performants. Par contre, aucune recherche empirique ne s'est intéressée à ces instruments, alors qu'ils sont implantés systématiquement dans les banques dans le but de répondre à leurs obligations. Il devient donc indispensable de s'y attarder afin de comprendre et de réellement saisir les pratiques de surveillance dans le cadre de la lutte à l'argent sale au sein des banques. Il est d'autant plus important de s'intéresser à ces outils technologiques, en matière de surveillance, à l'ère du *Big Data*.

Parallèlement, des écrits scientifiques se sont penchés sur l'émergence du *Big Data*, sur les technologies de surveillance et les algorithmes en sécurité, mais également dans plusieurs autres domaines scientifiques, tels que la santé. En revanche, très peu d'écrits portent sur le *Big Data* et l'utilisation des algorithmes par les banques à l'égard de la lutte au blanchiment d'argent et au financement du terrorisme. « À l'heure actuelle, l'appropriation des nouvelles technologies, et notamment des instruments algorithmiques à l'ère du big data, constituent aussi et surtout une dimension à part entière du processus quotidien de

production de sécurité. » (Amicelle, 2019, p.19). À cet égard, il devient donc important de s'attarder à ces technologies et instruments dans le cadre de la lutte au blanchiment d'argent et au financement du terrorisme, et ce, au sein des banques. D'autre part, bien que « L'intégration d'instruments automatisés [ait] eu un effet important sur l'organisation du travail interne des banques et la transformation des pratiques. » (Favarel-Garrigues, Godefroy et Lascoumes, 2009, p 201.), peu de littérature s'est penchée sur l'implantation de technologies au sein d'une banque : Quels sont les défis ? ; Comment les pratiques changent-elles ? ; Quelles sont les résistances ?

Compte tenu de ces lacunes dans la littérature actuelle, cette recherche aura pour objectif de répondre à la question suivante : Dans quelles mesures les nouveaux instruments algorithmiques implantés au nom de la lutte au blanchiment d'argent et au financement du terrorisme font une différence en matière de surveillance au sein des banques canadiennes ? Il s'agit donc de s'intéresser à l'implantation de technologies au sein des banques en matière de lutte au blanchiment d'argent et au financement du terrorisme et leurs impacts ; en quoi ces instruments transforment les pratiques. « Tenir compte des processus d'appropriation des nouvelles technologies est crucial pour être en mesure de (mieux) comprendre les pratiques de policing et de sécurité. » (Amicelle, 2019, p.19).

Cette recherche est donc pertinente du point de vue scientifique, mais celle-ci est également d'intérêt pour les praticiens. Effectivement, les résultats de cette recherche pourront entre autres permettre aux praticiens de cerner les écueils possibles lors de l'implantation de technologies au sein d'une banque et d'ainsi pouvoir y remédier. En effet, selon Rogers (2003), l'implantation de plusieurs innovations fut peu éloquente, d'où l'intérêt de mieux comprendre comment introduire de façon efficace les technologies informatiques. De plus, les résultats pourront également être utilisés par leurs homologues dans le domaine du *policing*.

Enfin, cette recherche permet également de se pencher sur le cas des banques canadiennes dans la lutte au blanchiment d'argent et au financement du terrorisme, alors qu'une forte partie de la littérature porte sur les banques américaines et européennes.

CHAPITRE 3 – CADRE THÉORIQUE

Cette recherche vise à étudier l'implantation de nouveaux dispositifs dans la lutte au blanchiment d'argent et au financement du terrorisme au sein des banques canadiennes. Plus précisément, cette recherche tente de répondre à la question précédemment mentionnée, soit de quelles façons ces outils technologiques font une différence dans les pratiques. Pour ce faire, au-delà du matériel empirique qui sera analysé, l'étude de Le Bourhis et Lascoumes (2014) sur les résistances aux instruments de gouvernement ainsi que l'étude de Amicelle, Aradau, et Jeandesboz (2015) sur les instruments en matière de sécurité seront utilisées comme cadre théorique.

L'étude de Le Bourhis et Lascoumes (2014) porte sur les résistances aux instruments de gouvernement, et ce, à différentes étapes de la production de l'action publique, lesquelles ont d'ailleurs été peu analysées. Le Bourhis et Lascoumes (2014) mettent donc de l'avant trois espaces de résistance : la conception de l'instrument, sa mise en œuvre et son appropriation par les utilisateurs. De prime abord, les auteurs soulignent que des affrontements et des frictions peuvent se former lors de la formulation de l'instrument entre les acteurs responsables de la conception, opposant différentes opinions et expertises (Le Bourhis et Lascoumes, 2014). La mise en œuvre et l'appropriation d'un instrument peuvent également mener à des résistances, que ce soit individuelles ou organisationnelles, telles que des oppositions aux changements (Le Bourhis et Lascoumes, 2014). Enfin, les comportements des utilisateurs et leur rapport aux programmes, lequel guide leurs conduites, offrent aussi un espace de résistance (Le Bourhis et Lascoumes, 2014).

Le Bourhis et Lascoumes (2014) mettent également de l'avant certaines formes de résistance et de pratiques d'opposition. « […] [L]a contestation des instruments est parfois une forme de prise de parole (*voice*), tandis que l'*exit* peut s'appliquer aux activités de contournement, de détournement et de neutralisation des instruments […] ». (Le Bourhis et Lascoumes, 2014). Parallèlement, Amicelle, Aradau, et Jeandesboz (2015) soulignent que les utilisateurs peuvent faire usage d'opérations de détournements moins visibles et peuvent modifier, influencer ou abandonner un dispositif sociotechnique. De plus, les

acteurs sociaux peuvent utiliser les instruments de sécurité à différentes fins que celles initialement prévues : les banques utilisent davantage les dispositifs de surveillance financière à des fins de protections légales et réputationelles, plutôt qu'à des fins de *policing* (Amicelle, Aradau, et Jeandesboz, 2015).

Par ailleurs, Amicelle, Aradau, et Jeandesboz (2015) soulignent que la force d'action des instruments de sécurité dépend des processus de production, de traduction, de circulation, d'appropriation, d'expérimentation ou de résistance. « Le processus dynamique de "dialogue" » entre un dispositif sociotechnique et un contexte d'action spécifique peut produire des effets imprévus et inattendus (Amicelle, Aradau, et Jeandesboz, 2015). La force d'action se développe en relation avec les acteurs qui les utilisent. Par conséquent, les concepteurs et les décideurs ne peuvent prévoir tous les effets préalablement (Amicelle, Aradau, et Jeandesboz, 2015). D'autre part, les instruments implantés (dé)stabilisent l'équilibre des pouvoirs entre les segments organisationnels en modifiant les routines considérées comme acquises, les relations entre les rôles, la division du travail, etc. (Amicelle, Aradau, et Jeandesboz, 2015).

Dans le cadre de la présente recherche, trois espaces seront pris en considération : la formulation des instruments et le processus de décision quant à la technologie désirée, la mise en œuvre de celle-ci et l'appropriation de cette technologie par les utilisateurs. Ainsi, ces espaces permettront d'analyser la façon dont la technologie, en tant qu'instrument de sécurité, est implantée et appropriée, ainsi que ses effets et les enjeux qu'elle soulève lorsqu'elle est en contact avec les utilisateurs et le contexte d'action spécifique, soit la banque.

CHAPITRE 4 – MÉTHODOLOGIE

1. La méthodologie qualitative

Dans le cadre de cette recherche, une méthodologie qualitative fut privilégiée afin de répondre au présent objectif de recherche. Cette approche méthodologique permet notamment d'intégrer plusieurs perspectives, de décrire un processus et d'apprendre comment les évènements sont interprétés par les différents acteurs du milieu (Weiss, 1994). De plus, cette approche offre la possibilité d'obtenir une description de la structure ou du fonctionnement d'une organisation, dans le cas présent, de la banque (Weiss, 1994). Ainsi, différentes descriptions, interprétations et opinions peuvent être obtenues sur un évènement (Weiss, 1994) ; concrètement, dans le cadre de cette recherche, l'approche qualitative permet d'obtenir l'interprétation de plusieurs acteurs à l'égard de l'implantation d'un nouvel outil technologique au sein de leurs pratiques. Elle permet d'autant plus d'obtenir un accès privilégié au fonctionnement et aux pratiques de cette organisation.

L'analyse qualitative des données permet de dégager le sens des actions et des expériences humaines. Elle permet également de saisir les interprétations et descriptions de ces actions (Paillé et Mucchielli, 2016). Contrairement à l'analyse quantitative, l'analyse qualitative permet de comprendre et d'interpréter les pratiques et l'expérience des acteurs ; ce qui rejoint directement l'objectif de la présente recherche (Paillé et Mucchielli, 2016). De fait, cette recherche s'intéresse à l'expérience des acteurs et plus précisément à connaître les changements occasionnés au sein de leurs pratiques et leurs perceptions vis-à-vis ces changements.

Afin de procéder à la collecte de données, des entrevues semi-dirigées ont été réalisées auprès de différents acteurs du milieu étudié. Des entrevues semi-dirigées furent privilégiées comme méthode qualitative, puisqu'elles sont essentielles en vue de connaître l'action publique, et ce, dans une dimension historique ou synchronique (Pinson, G. et Sala Pala, 2007). Effectivement, « L'usage compréhensif [de l'entretien] ouvre la voie à l'analyse des pratiques quotidiennes des acteurs des politiques publiques et des

représentations qui les orientent. » (Pinson, G. et Sala Pala, 2007, p. 597). De plus, l'entretien permet d'avoir accès aux processus d'une « intervention publique ou d'une décision » (Pinson, G. et Sala Pala, 2007, p.577). Les entrevues semi-dirigées permettent donc, d'une part, d'obtenir l'accès aux pratiques quotidiennes des acteurs et, d'autre part, l'accès au processus étudié dans son ensemble, soit les actions et décisions successivement prises au cours de la sélection, l'implantation et l'appropriation d'une nouvelle technologie. D'autant plus, « […] les entretiens permettent de comprendre trois types de choses : les contraintes du système ; les relations sociales, la culture d'une institution, les valeurs ; et enfin, la résistance aux contraintes. » (Pinson, G. et Sala Pala, 2007, p. 593). La compréhension de ces dimensions est d'ailleurs essentielle afin d'étudier l'espace d'appropriation des utilisateurs. De plus, l'entretien semi-directif cherche à accéder aux pratiques et représentations des acteurs sociaux (Pinson, G. et Sala Pala, 2007) ; ce qui rejoint l'objectif de la présente recherche. Enfin, pour le chercheur, il s'agit d'un outil rapide et économique qui offre des données de qualité pour l'analyse d'un champ spécifique, telle qu'une banque (Pinson, G. et Sala Pala, 2007).

2. La collecte de données

Les entrevues semi-dirigées furent réalisées par le directeur de la présente recherche, Anthony Amicelle, et ce, auprès de huit personnes travaillant au sein d'une banque canadienne. À des fins de confidentialité, le nom de la banque est préservé. Ces entrevues ont été réalisées à partir de certains thèmes généraux et plus spécifiques préalablement établis et ont été d'une durée d'environ une heure pour chacune d'entre elles. Les entrevues ont été enregistrées afin d'éventuellement en faire la transcription ; cette méthode permet d'être complètement attentif aux propos de la personne tout au long de l'entretien et ainsi éviter de devoir se préoccuper de noter les échanges. La transcription permet d'autant plus une analyse plus approfondie des propos des répondants et de saisir des composantes particulières lors de l'analyse des transcriptions. (Weiss, 1994).

Les entretiens ont été effectués auprès de huit personnes, lesquelles travaillent au sein de la même banque. Bien que huit personnes aient participé, sept entrevues ont été réalisées auprès des personnes suivantes : 1) Deux membres de la direction anti-blanchiment ; 2) Un

de ces deux membres de la direction anti-blanchiment ; 3) Une consultante en gestion de changement ; 4) Un représentant TI de la banque ; 5) Un employé chargé de faire l'accompagnement en intelligence d'affaires ; 6) Un employé ayant surtout travaillé sur le paramétrage des alertes ; et 7) Deux membres de l'équipe chargée de traiter les alertes automatisées. Ces entretiens ont été réalisés au cours de la dernière année, et ce, sur le lieu de travail des participants.

3. Les limites méthodologiques

Cette recherche comporte certaines limites méthodologiques. De prime abord, seulement une banque fut considérée pour la recherche, ce qui pose des limites quant à la généralisation des résultats de la recherche. De fait, ceux-ci ne peuvent se targuer d'être exhaustifs, mais offrent en revanche des conclusions intéressantes et pertinentes pour l'organisation, en plus de combler des lacunes dans la littérature. De plus, les résultats mettent en lumière une situation contemporaine à laquelle d'autres banques sont confrontées et représentent ainsi une certaine part de leur réalité.

Parallèlement, les entrevues furent réalisées auprès de huit personnes occupant un poste au sein de la banque ; les résultats sont donc limités quant à leur généralisation en ce sens également. Toutefois, les personnes ont notamment été choisies en fonction de cette limite et sont donc des personnes qui ont un rôle déterminant dans l'implantation de l'instrument technologique au sein de l'organisation, et ce, à plusieurs niveaux du processus. Par conséquent, l'apport de ces personnes en fonction de leurs différents rôles et expériences vient optimiser les résultats de la recherche. Il convient d'autant plus de souligner qu'un nombre élevé d'entretiens n'est pas proportionnel à la qualité de la recherche (Pinson, G. et Sala Pala, 2007).

Enfin, il y a la possibilité d'une part, que les acteurs dissimulent certains faits ou omettent de divulguer certaines informations lors des entretiens (Pinson, G. et Sala Pala, 2007 ; Weiss, 1994). D'autre part, les répondants peuvent avoir oublié certaines étapes d'un processus venant ainsi biaiser les résultats (Pinson, G. et Sala Pala, 2007). Par contre, dans le cadre de cette recherche, les entretiens ont été effectués auprès de personnes ayant des

rôles variés ; les mêmes informations, dans différents contextes, reviennent généralement dans plus d'un entretien, venant ainsi corroborer les informations obtenues. De ce fait, il est possible de croire que les données collectées sont exactes.

CHAPITRE 5 – ANALYSE DES RÉSULTATS

La présente recherche s'intéresse aux changements en matière de surveillance, au sein des banques canadiennes, apportés par l'implantation d'instruments algorithmiques, et ce, dans une perspective de lutte au blanchiment d'argent et au financement du terrorisme. La banque étudiée dans le cadre de cette recherche a récemment procédé à l'implantation d'un logiciel de détection algorithmique en matière de surveillance financière. Alors qu'auparavant la surveillance transactionnelle était dirigée exclusivement vers les clients à risque, la surveillance transactionnelle est désormais dirigée vers tous les clients de la banque. Ce logiciel algorithmique analyse les transactions financières des clients et génère des alertes lors de la détection de transactions a priori suspectes, lesquelles seront traitées par un analyste et envoyées, le cas échéant, au Centre d'analyse des opérations et déclarations financières du Canada (CANAFE).

1. La formulation de l'instrument

1.1. Le processus de décision : les motivations à l'égard de l'implantation

L'implantation d'un nouvel instrument technologique au sein d'une organisation peut être motivée par une diversité de facteurs (Rogers, 2003). De fait, plusieurs raisons ont été mentionnées par les participants, lesquelles ont mené à l'implantation d'une nouvelle technologie au sein de la banque : un logiciel de détection algorithmique. De prime abord, certains participants ont évoqué les exigences réglementaires auxquelles les banques sont assujetties. Effectivement, une réforme du régime canadien, survenue en 2008, exige désormais une surveillance en continu pour les clients de l'institution : toutes les relations d'affaires doivent être surveillées et plus uniquement les clients représentant un risque élevé. Selon la logique à l'œuvre, il s'avère important de surveiller tous les clients de la banque, car bien qu'une personne n'ait pas de passé criminel et qu'elle ne présente pas un risque élevé, celle-ci peut néanmoins avoir un comportement transactionnel considéré comme suspect. Par ailleurs, la non-conformité avec cette exigence réglementaire est passible d'une pénalité financière importante pour les banques concernées. De plus, cette omission de se conformer à la loi peut également poser un risque réputationnel pour la

banque ; les examens du régulateur (CANAFE) et autres audits effectués en interne sont de plus en plus fréquents à cet effet. Selon cette même logique, la surveillance engendrée par cette exigence réglementaire apporte une plus-value à la banque, notamment par l'envoi de déclarations plus rigoureuses au CANAFE et par l'interception de transactions qui n'auraient été détectées auparavant.

De surcroît, l'instrument fut implanté afin de répondre à un enjeu opérationnel pour l'institution. Effectivement, bien qu'il ne s'agisse pas d'une exigence réglementaire d'acquérir un système automatisé, en raison du volume important de transactions à traiter, la banque a dû opter pour un tel système :

> « On a quand même regardé l'idée de, est-ce qu'on signe pas [le logiciel], puis je demande aux employés de première ligne de bonifier tous les contrôles manuels et humains qui sont en place pour atteindre l'objectif, puis arriver avec le même niveau. Puis honnêtement, t'as pas besoin d'analyser longtemps que ça prendrait une armée formée avec des vues systématiques » (Entrevue 7).

Conséquemment, un système automatisé a été appréhendé comme plus efficient que de procéder au recrutement de centaines, voire de milliers de personnes pour effectuer ce travail, d'autant plus que des problèmes spécifiques découlent de l'analyse humaine. En effet, d'une part, l'analyse effectuée varie selon chaque personne et résulte donc en la détection de divers types de transactions. D'autre part, certains patterns de blanchiment d'argent ne peuvent être détectés à l'œil nu en raison de leur complexité et/ou de leur faible visibilité au sein du volume transactionnel quotidien. La décision d'opter pour un système automatisé est par conséquent motivée par des raisons budgétaires et d'efficacité opérationnelle.

Finalement, cet instrument a été intégré dans une perspective de conformité et de saines gestions des risques. En effet, cette surveillance en continu de tous les clients est perçue comme permettant de renforcer le régime et ainsi protéger les clients, voire les citoyens :

> « On s'entend que même s'il n'y avait pas d'exigences, probablement que [nom de la banque] l'aurait mis en place, comme d'autres institutions mettent des choses en place, pour gérer notre risque et aider le régime. Mais à la base du pourquoi là, c'était parce que c'était une exigence réglementaire » (Entrevue 7).

Ainsi, au-delà des motifs, mentionnés précédemment, quant à l'implantation d'un nouvel instrument technologique, l'exigence réglementaire apparaît tout de même comme le facteur ayant prévalence. Par contre, l'implantation d'un système automatisé pour satisfaire ces exigences était un choix systématique pour la banque, en raison de l'importance du volume transactionnel.

1.2. Le processus de sélection de l'instrument : le choix du logiciel

Plusieurs raisons ont ainsi mené à la décision d'implanter un instrument algorithmique au sein de la banque. Subséquemment, un processus de sélection quant à la technologie désirée s'ensuit. Les participants ont d'ailleurs mentionné une multitude de critères de sélection qui ont mené vers le choix de la technologie retenue. D'emblée, l'instrument devait avoir la capacité de gérer un large volume de transactions financières afin de répondre à une pertinence opérationnelle et aux besoins de l'institution. Il devait également être apte à fonctionner en conformité avec le régime canadien et ses spécificités. À cet égard, il devait avoir la capacité de traiter des données en français et en anglais, dû aux exigences canadiennes relatives à la langue. L'instrument devait donc ultimement maximiser les exigences et les besoins de la banque, et ce, à un rapport qualité/prix raisonnable.

Ainsi, le fournisseur sélectionné répondait à ces critères et aux besoins d'affaires de la banque, d'autant plus qu'il offrait plusieurs modules, dont celui en ce qui a trait à la surveillance automatisée des transactions. De ce fait, sélectionner ce fournisseur était favorable en termes de synergie pour la banque, étant donné qu'elle pouvait bénéficier de tous les modules issus du même fournisseur. Enfin, en raison des spécificités de la banque et de son statut, le fournisseur devait avoir de bonnes capacités technologiques, être bien implanté et important dans l'industrie : les compagnies d'envergure risquent habituellement moins de cesser leurs activités que les plus petites entreprises, évitant ainsi de devoir recommencer ce processus de sélection.

Par ailleurs, les processus de décision et de sélection s'inscrivent dans un milieu en perpétuelle évolution. En effet, certains participants soulignent que dans le cadre de la lutte au blanchiment d'argent et au financement du terrorisme, la banque doit constamment

s'adapter à des changements réglementaires, organisationnels et technologiques. De nouvelles réglementations imposées par le gouvernement, qui surviennent aléatoirement, obligent la banque à faire des restructurations afin de s'y adapter, et ce, sans nécessairement avoir de nouveaux budgets pour y arriver. L'organisation et la technologie sont également en continuelle évolution, ce qui nécessite des ajustements pour la banque. À cet effet, bien que l'outil technologique sélectionné réponde actuellement aux besoins de la banque, il est possible que le processus de sélection soit à recommencer dans quelques années avec la venue de nouveaux outils technologiques plus sophistiqués et performants.

1.3. La conception de l'outil : la paramétrisation

Lorsque le logiciel est sélectionné comme étant celui qui correspond aux besoins de la banque et qui optimise les ressources disponibles, l'outil doit être configuré à cet effet. Le logiciel comprend plusieurs règles de détection, qui correspondent à des comportements financiers suspicieux ; ces algorithmes détectent ces comportements suspicieux et génèrent des alertes. Bien que le logiciel soit initialement accompagné d'une centaine de règles, développées par des mathématiciens et des « data scientists » maîtrisant le domaine bancaire, celles-ci n'ont pas toutes été intégrées. De fait, devant ce volume important de règles, toutes n'étaient pas unanimement considérées comme pertinentes ou applicables à la banque. D'autant plus qu'un fort volume de règles résulte également en un volume important d'alertes générées : non seulement il n'est pas possible de toutes les traiter, mais celles qui sont pertinentes sont plus difficilement repérables, noyées dans la masse. Toujours dans cette perspective, les règles doivent aussi être choisies en fonction des produits et services de la banque. Par conséquent, bien que les règles du modèle de base offrent un bon départ pour une banque, il est inefficace d'intégrer toutes les règles de détection proposées. Un travail important devait donc être fait afin d'optimiser l'outil pour les besoins de la banque. Pour ce faire, les risques doivent être établis et il convient ainsi de choisir les règles de détection nécessaires pour gérer ces risques. Il fallait également que la banque se questionne par rapport à la présence et la disponibilité des données pour faire fonctionner ces règles et qu'elles soient productives.

Ainsi, les règles sont des algorithmes, soit, dans le cas présent, des calculs purement mathématiques renvoyant à une « série d'instructions permettant d'obtenir un résultat » (Cardon, 2015, p.7). Par conséquent, afin que ces règles puissent fonctionner, des seuils ont dû être établis pour chacune d'entre elles : le montant, l'occurrence, l'endroit, etc. Cette paramétrisation est fort importante étant donné que les seuils établis détermineront les transactions qui seront détectées et éventuellement analysées. Si un seuil est réglé trop haut, certaines transactions ne seront pas décelées, alors que si le seuil est trop bas, un volume important de transactions est détecté et donc un fort volume d'alertes est généré, dont des faux positifs. La banque doit alors s'assurer qu'il n'y a pas d'alertes de générées en trop, puisqu'elles deviennent inefficaces le cas échéant. D'ailleurs, un participant souligne que : « Le but là, c'est pas mettre des seuils à un niveau où on est capable de gérer le volume, mais c'est de mettre des seuils là où ça va générer de la valeur ajoutée pour l'organisation, puis pour le régime » (Entrevue 1). Il s'agit donc d'un travail complexe pour lequel la banque a entre autres sollicité l'expertise des personnes qui font les déclarations, afin de connaître les patterns observés en matière de blanchiment d'argent et de financement d'activités terroristes. Par ailleurs, la paramétrisation du logiciel nécessite de continuels ajustements, ce que la banque avait d'ailleurs anticipé :

> « Fait que trouver le bon seuil, trouver le bon niveau euh on est encore en train de, d'ailleurs depuis qu'on a livré on a fait de multiples modifications à nos seuils, à nos occurrences, à nos, à toutes nos règles, parce que les opérations nous reviennent avec des points d'interrogation. Tsé quand on a 0.5 % de productivité ou 1 % de productivité sur une règle euh. » (Entrevue 1)

La paramétrisation est donc un processus laborieux où la banque doit tenter de trouver les seuils et les règles idéals pour ne pas laisser passer des transactions de blanchiment d'argent et de financement d'activités terroristes, et ce, sans toutefois générer un volume trop important d'alertes.

De plus, un pointage est attribué à chacune des règles, lequel est décidé en fonction des besoins d'affaires de la banque. Le pointage est associé au comportement : pour telle occurrence, tel pointage est attribué et ainsi de suite. Lorsqu'un certain pointage est atteint, une alerte sort automatiquement et doit être traitée par des analystes. Par exemple, une pondération est faite selon le niveau de risque posé par les clients, ce qui ajoute des points

aux comportements effectués par ces membres. Il s'agissait donc aussi d'un besoin d'affaires pour la banque de surveiller encore plus rigoureusement qu'avant les transactions des clients à risque. D'ailleurs, des revues périodiques seront effectuées pour ces personnes à risque. Afin d'établir le risque posé par une personne, un calcul est fait à partir des facteurs de risque et un niveau de risque est dès lors attribué en fonction du résultat obtenu. Si un changement se produit et un saut de niveau est fait, une alerte est générée, c'est-à-dire lorsqu'une personne devient à risque ou augmente de niveau de risque à la suite d'un comportement. Par exemple, une personne pour laquelle une déclaration d'opération douteuse (DOD) est envoyée à CANAFE pour la première fois devient à risque, ce qui génère une alerte.

Parallèlement à ce travail de conception, un travail de *mapping* concernant les codes des transactions a dû être effectué. Les codes sont utilisés à l'interne afin d'identifier le type de transactions. Bien que la banque avait sa propre façon de coder les transactions, elle a dû les « traduire » et les rendre compatibles selon les codes du logiciel, afin que les règles puissent fonctionner. Il s'agissait d'un travail présenté comme colossal, car la règle fonctionne avec les transactions ; elles doivent donc être correctement codées pour que la règle fonctionne et pour éviter les erreurs manifestes.

Ainsi, ce logiciel implanté dans le cadre de la lutte au blanchiment d'argent et au financement du terrorisme utilise des algorithmes afin de déceler des transactions suspicieuses. Or, il s'agit uniquement de calculs mathématiques qui opèrent à partir de grandes bases de données, sans prendre en considération l'aspect humain et comportemental (Cardon, 2015). À cet effet, aucun système de surveillance ne peut capter cet aspect, alors qu'il serait nécessaire pour discerner certains criminels : « C'est purement mathématique. Tandis qu'il y a une grosse proportion, euh, des informations dont on aurait de besoin pour capter ces criminels là, qui est pas métrique là, qui est humain là. » (Entrevue 1). À titre d'exemple, certains comportements considérés comme des indicateurs d'anormalité, tels qu'un client qui insiste pour que la transaction soit faite rapidement, ne peuvent être pris en considération par des instruments technologiques (Amicelle et Iafolla, 2017).

Toutes ces décisions en ce qui a trait aux choix de règles et de seuils ont été prises avant de voir les données disponibles, c'est-à-dire avant même de savoir si les règles et les seuils allaient pouvoir fonctionner congrûment avec les données. Conséquemment, par la suite, une vérification devait être faite à cet effet, pour voir la compatibilité des règles avec les données de la banque. Celle-ci devait donc s'assurer que des données étaient disponibles pour que la règle fonctionne et vérifier que les règles sont productives et apportent une plus-value. La banque ne souhaitait pas livrer une version finale du logiciel ; il aurait d'ailleurs été utopique de prétendre pouvoir développer quelque chose de définitif. Ainsi, le logiciel était plutôt évolutif et nécessitait plusieurs étapes de paramétrisation et d'amélioration.

2. La mise en œuvre de la technologie au sein de la banque

2.1. La préparation à l'implantation d'une nouvelle technologie

L'implantation du nouveau logiciel algorithmique exigeait préalablement une organisation de la part de la banque. Dans un premier temps, une nouvelle équipe, composée d'analystes, devait être créée pour travailler avec l'outil, plus précisément afin de traiter les alertes générées par ce dernier. Les analystes sélectionnés proviennent de différentes équipes internes de la banque, lesquels connaissent, d'une part, le blanchiment d'argent et, d'autre part, la banque et ses spécificités, facilitant ainsi les formations. Par conséquent, la formation offerte aux analystes est plus technique et donc spécifique à l'outil. Parallèlement, les personnes sélectionnées devaient avoir une expérience en analyse et avoir un bon discernement en ce qui a trait au blanchiment d'argent. De plus, les personnes devaient être réceptives face à ce changement de culture organisationnelle, occasionné par le logiciel implanté, et face aux nouveaux enjeux engendrés par cette transformation. Bien qu'il s'agisse d'un changement important, celui-ci n'était pas imposé aux analystes, lesquels pouvaient volontairement participer à ce projet. Par conséquent, ces personnes étaient conscientes et enthousiastes par rapport à ce changement, évitant ainsi toute forme de résistance (Chan, 2001 ; Éricson et Haggerty, 1997 ; Rogers, 2003). Enfin, la banque devait sélectionner parmi des candidats qui œuvrent déjà au sein de l'organisation, il était alors possible de savoir qui serait compétent dans ces nouvelles tâches. Ainsi, la banque a

pu former une équipe performante composée de personnes engagées et emballées à l'idée de travailler avec ce nouvel instrument.

Dans un deuxième temps, la banque a eu recours à un accompagnement de transformation, afin de les assister dans l'implantation d'une nouvelle technologie. D'emblée, cette personne externe devait s'approprier la complexité de l'institution et son fonctionnement, dans le but de procéder à l'accompagnement conformément aux exigences. La première étape était d'identifier les parties prenantes à ce changement, soit les analystes et les gestionnaires, alors que la deuxième étape consistait en l'identification des impacts ; la gestion de changement sera alors faite en regard de ces éléments. Dans le cadre de l'implantation du nouveau logiciel, il était possible de prévoir un impact technologique énorme ainsi que des impacts sur la structure organisationnelle. À cet effet, la banque a informé les employés qu'un changement structurel allait se produire, c'est-à-dire que les équipes n'allaient plus travailler en vase clos, mais allaient désormais être dépendantes les unes des autres ; il était important pour la banque d'être transparente dans le cadre de cette transformation et ainsi leur expliciter ce à quoi s'attendre. Ainsi, les équipes qui travaillent avec les différents modules du logiciel auront accès à la même plateforme, ce qui leur permettront, entre autres d'avoir accès à toutes les alertes des modules. De ce fait, les équipes seront plus interconnectées et seront amenées à interagir entre elles.

De plus, des ateliers en gestion de changement ont été réalisés, lesquels portaient sur deux volets. Le premier atelier portait sur la gestion du changement et sur la façon dont celui-ci doit être vécu par les analystes. L'atelier permettait notamment de normaliser leur anxiété à l'égard du changement :

> « T'as une partie de ben de comprendre un petit peu ce que c'est de vivre un changement, parce que tu sais tu peux le dire, mais c'est différent de vraiment le vivre. […] c'est plutôt de te faire comprendre qu'on n'est pas en train de te dire qu'il faut que tu aimes le changement, il faut que tu sois super content et tout, mais plutôt que c'est normal que tu sois mal à l'aise, c'est normal que tu sois stressé et en fait […] ». (Entrevue 5).

D'ailleurs, l'accompagnement des analystes était important dans cette transition. Le deuxième atelier concernait le travail d'équipe, qui visait à aider les analystes à travailler ensemble plus efficacement et à leur permettre de développer des synergies entre les

équipes. Étant donné que ces personnes proviennent de différentes équipes internes, ces ateliers permettaient aussi d'éviter qu'elles soient en rivalité. Enfin, dans une perspective d'efficacité, une dynamique d'équipe apparaît fondamentale, et ce, plus particulièrement lorsqu'il y a une pression exercée sur l'équipe, tel est le cas pour ce logiciel.

Dans un dernier temps, des formations ont dû être créées dans le cadre de la mise en œuvre du logiciel : « […] la formation c'est justement la partie visuelle, la plupart des gens voient vraiment ça, puis en terme de bénéfices, je te dirais que de retombées positives, tu dois avoir 20 % des bénéfices qui sont faits grâce à la formation et 80 sur tout le reste que tu fais avant » (Entrevue 5). En effet, l'accompagnement en gestion de changement implique une approche personnalisée en amont avec les gestionnaires d'une part, et, d'autre part, des formations. Une approche en amont avec les gestionnaires était primordiale afin, entre autres choses, de cerner leurs attentes. De plus, puisqu'il s'agissait d'un changement majeur, un atelier avec les gestionnaires aux opérations a été réalisé, lequel portait sur la façon de faire en tant que gestionnaire. Ultérieurement, plusieurs personnes se sont rassemblées afin de préparer des formations qui répondent aux exigences des gestionnaires et qui sont optimales pour les analystes. À cet égard, les formations devaient guider la réflexion des analystes vers un traitement optimal et rapide des alertes. En effet, lors d'une implantation antérieure d'un logiciel par la banque, des recherches trop approfondies et jugées inutiles étaient effectuées par les analystes, ce qui prenait beaucoup de temps. Par conséquent, la banque voulait éviter qu'une situation similaire se reproduise. Ainsi, la première session présentait le projet dans son ensemble et la deuxième session présentait les règles. Suivant ces formations, des périodes de temps ont été allouées afin de tester les règles : une règle était présentée aux analystes et ceux-ci devaient traiter les alertes générées par cette règle. Les analystes n'avaient pas d'objectifs à atteindre à ce moment, ce qui leur permettait de bien comprendre leur rôle, la technologie et de bien se les approprier. Un objectif sous-jacent de ces périodes était de créer une dynamique d'équipe : « Ils s'aidaient entre eux et ça leur permettait aussi de s'approprier le module, mais aussi de créer leur dynamique d'équipe » (Entrevue 5). Ces périodes permettaient également aux analystes de connaître le gestionnaire, qui était connu seulement par la moitié de l'équipe.

2.2. L'introduction de la technologie

Afin de procéder à l'implantation de ce nouvel instrument algorithmique, la banque a eu recours à un « intégrateur de systèmes technologiques », qui a participé au processus de sélection. Les représentants de cet intégrateur, en tant qu'entreprise et qu'employés spécialisés, connaissaient bien l'outil et avaient procédé à son implantation à plusieurs reprises. Par conséquent, l'intégrateur pouvait donner des recommandations et suggérer quels seuils et quelles règles choisir en fonction de ce que d'autres banques avaient sélectionné. Par contre, les règles proposées par ce dernier n'ont pas nécessairement été toutes intégrées, puisqu'il ne possède pas une aussi bonne connaissance du marché canadien que la banque. Recourir à un intégrateur permettait également de repérer la source des problèmes rencontrés ainsi que de prévenir certains comportements, afin d'éviter d'éventuels enjeux : « Puis ça [recourir à un intégrateur], ça a été vraiment vraiment très aidant parce qu'eux aussi sont passés par là. On a des enjeux, tout de suite ils peuvent nous dire : "oui, c'est à cause de telle raison ou faites pas ça parce que vous allez avoir tel enjeu." Ça ça a été vraiment très très aidant » (Entrevue 2).

Les règles de détection ont donc été choisies avec l'intégrateur, et ce, plusieurs mois avant d'avoir accès aux données de production, c'est-à-dire aux transactions des clients, soit les avoirs, les actifs et les passifs, qui sont des données très sensibles. De fait, la banque était sceptique d'autoriser l'accès aux programmeurs et consultants à ces données sensibles. Éventuellement, les règles de détection devaient donc être essayées afin de s'assurer que les alertes correspondent et qu'elles ne soient pas générées en trop ; le cas échéant, les règles et les alertes sont inefficaces. Cet essai permettait également de s'assurer que les règles correspondent aux besoins de la banque et qu'elles génèrent des bénéfices.

Ainsi, cette structuration a permis de procéder à certaines corrections. De prime abord, lors de la première version, un important volume d'alertes était généré, ce qui aurait nécessité beaucoup plus d'analystes pour effectuer le travail. En effet, certaines règles n'avaient pas été peaufinées et plusieurs règles apportaient des faux positifs. Par conséquent, certaines règles ont été désactivées et des seuils ont été modifiés afin de rendre les règles productives. Parallèlement, certains produits surveillés, dont les épargnes internes, ont mené la banque

à se positionner par rapport à la nécessité et la pertinence de les contrôler. Enfin, la codification a dû être améliorée, étant donné que certains codes ne reflétaient pas nécessairement une réelle situation, où entre autres un chèque était considéré comme de l'espèce, ce qui faussait l'exercice de détection.

2.3. Les enjeux associés à l'implantation d'une nouvelle technologie

L'implantation d'un instrument algorithmique au sein de la banque donne lieu à certains enjeux. D'emblée, des limites budgétaires s'imposent dans le cadre de l'implantation du logiciel. Bien que la lutte au blanchiment d'argent et au financement du terrorisme soit fondamentale pour une banque, il ne s'agit pas de leur fonction initiale ni principale et est plutôt perçue comme une source de coût. Un budget est prévu annuellement pour la lutte au blanchiment d'argent et au financement du terrorisme, lequel doit être respecté dans le cadre des activités relatives à cette lutte. Ainsi, le logiciel a été sélectionné notamment en fonction des ressources financières disponibles. De même, le nombre d'analystes, soit 16, découle des ressources disponibles. De ce fait, la paramétrisation de l'outil doit prendre en considération le nombre d'analystes, afin de générer un nombre d'alertes qui pourra être analysé par ces derniers.

Par ailleurs, une problématique qui revient de façon récurrente dans les entrevues se situe au niveau de la qualité des données. Tout d'abord, une mauvaise utilisation des codes par les employés de première ligne a été décelée. En effet, certains employés de succursales bancaires n'utilisent pas correctement les codes de transactions et l'information est par conséquent rentrée inadéquatement dans le système. De plus, certains utilisent ces codes de façon manuelle afin de simplifier leur travail, ce qui, de fait, impacte les systèmes de surveillance. De surcroît, les employés de première ligne ne sont pas conséquents dans la systématisation de l'information : la donnée est parfois accessible dans le système, parfois en format papier, et dans certains cas, tout simplement indisponible. Parallèlement, ce ne sont pas systématiquement les mêmes questions qui sont posées aux clients, d'autant plus que le volume de questions posées aux clients tente d'être réduit :

> « Puis on essaie de rendre l'expérience client plus facile, plus simple, donc on voudrait que les procédures d'ouverture de comptes se fassent plus rapidement, en posant le moins de questions possible. Mais tout ça va à l'encontre de ce que nous

> on a de besoin, avec le blanchiment d'argent, c'est-à-dire de collecter le plus d'information sur les membres clients pour être capable de les suivre, de les suivre, puis de comprendre leur pattern transactionnel, leurs habitudes » (Entrevue 1).

Enfin, d'un côté plus technique, les codes utilisés par la banque regroupent plusieurs types distincts de transactions, ce qui engendre un manque de précision par rapport aux données. Par exemple, le code pour un retrait au comptoir englobe un retrait, un retrait pour acheter une autre devise, de même que la prise de possession d'un chèque officiel. Ce problème relatif à la qualité des données a un impact sur la conformité. Par conséquent, ayant réalisé son ampleur, la banque a démarré des comités de la gouvernance relativement à ce problème. Toutefois, des efforts doivent également être faits par les employés de première ligne.

De même, un problème a été décelé par rapport à la régularité de l'information pour la donnée, soit la métadonnée. Lorsque des informations sont envoyées d'un système à un autre, des informations sont coupées lors du transfert. Ainsi, la donnée existe et est présente dans le système initial, mais elle est partiellement tronquée et donc perdue lorsqu'elle passe à un autre système. Par conséquent, dans le cadre de l'implantation du nouvel outil algorithmique, un enrichissement de données a dû être fait afin d'aller chercher des informations manquantes pour certaines règles. À cet égard, le niveau de certitude de l'enrichissement de données n'est pas toujours à 100 %. Conséquemment, les transactions ayant été bonifiées avec l'enrichissement de données ne sont possiblement pas précises à 100 %. Il s'agit actuellement d'un enjeu pour la banque qui ne possède pas de source autoritaire où toutes les informations se retrouvent. Le cas échéant, la banque pourrait aller chercher les données manquantes et éviter de devoir faire un enrichissement de données.

De plus, le *mapping* des transactions a posé problème lors de la l'implantation du nouveau logiciel. Les écueils décelés étaient techniques, tels que l'identification de comptes actifs comme comptes dormants et des remboursements de prêts crédits, soit des hypothèques, considérés comme des transactions « débit ». La banque a donc essayé de déceler toutes les erreurs relatives au *mapping*, car elles peuvent être problématiques, notamment dans le cas où un compte n'est pas pris en considération, alors qu'il doit l'être. Conséquemment, des correctifs ont été apportés au *mapping* du logiciel.

Par ailleurs, un participant a soulevé l'importance de la « segmentation » des populations. À cet effet, il est fondamental de surveiller et distinguer les clients très aisés et fortunés des clients moins nantis ; ce qui n'est actuellement pas le cas pour la banque. L'enjeu pour la banque est de trouver une source autoritaire de la banque de classification des clients, et ce, en fonction de la segmentation des clients. La segmentation des clients peut être faite avec plusieurs règles et de différentes façons, soit selon les revenus, les actifs, le volume transactionnel, etc. Toutefois, la banque n'a pas nécessairement accès à toutes ces données actuellement. De plus, les informations sur les membres doivent être à jour, telles que les informations relatives à l'emploi. D'un autre côté, l'ultra segmentation devient difficilement gérable, étant donné que des seuils différents doivent être établis pour chaque segmentation. Or, la banque travaille actuellement sur la segmentation des clients qui est un développement technologique requérant beaucoup d'efforts.

3. L'appropriation de la technologie par les utilisateurs

3.1. Les pratiques de surveillance algorithmique

L'implantation d'une nouvelle technologie au sein des pratiques bancaires nécessitait une longue préparation et un soutien externe lors de l'introduction. Ce travail en amont a notamment été réalisé afin d'aider l'appropriation de la technologie par les utilisateurs. En aval de ces préparatifs se trouve une logistique de travail méthodique pour les utilisateurs. À cet effet, deux niveaux d'analyse sont effectués à partir des alertes générées par le logiciel de surveillance. Ainsi, une analyse de l'intégralité des alertes est effectuée (analyse de premier niveau), laquelle résulte soit en la fermeture de l'alerte, c'est-à-dire en la conclusion d'un faux positif, soit en une analyse plus approfondie de l'alerte (analyse de deuxième niveau). Les recherches effectuées par l'analyse de deuxième niveau peuvent résulter en une Déclaration d'opération douteuse (DOD) au CANAFE.

Le logiciel de surveillance algorithmique génère les alertes durant la nuit, lesquelles sont ensuite assignées aux analystes. Généralement, les alertes assignées aux analystes ont été générées il y a 10 jours. À cet égard, les alertes doivent toutes être traitées dans un délai de 30 jours. Conséquemment, les alertes générées il y a plus longtemps sont normalement

celles analysées en premier ainsi que les alertes pour les membres à risque. L'attribution des alertes aux analystes est aléatoire, ce qui leur permet d'être familiers avec tous les types d'alertes. Les analystes de premier niveau traitent approximativement 30 alertes quotidiennement, pour lesquelles le traitement est d'environ 15 minutes ; dans bien des cas, il ne faut que 5 minutes pour fermer l'alerte. Avec le temps, les analystes deviennent plus expérimentés et reconnaissent les répétitions et certains patterns et ferment donc plus rapidement les alertes. Afin de procéder au traitement des alertes plus efficacement et rapidement, un arbre décisionnel a été conçu pour chaque règle, dans le but de supporter les analystes. L'arbre décisionnel présente donc plusieurs situations auxquelles les analystes peuvent être confrontés et les guide dans les procédures à suivre pour chacune d'entre elles.

Ainsi, ce traitement peut émaner en la fermeture d'une alerte, c'est-à-dire un faux positif : une alerte a été générée et à la suite de vérifications, rien de suspicieux requérant davantage d'analyse n'a été détecté. À cet effet, plus ou moins 90 % des alertes sont des faux positifs. Lorsque c'est le cas, une note justifiant sa fermeture est rédigée. Par conséquent, si une alerte similaire est générée, la note de fermeture de la précédente est disponible, ce qui accélère le processus. De plus, toutes les alertes analysées au premier niveau vont être déposées dans un dossier pendant 25 jours, permettant l'accumulation d'informations supplémentaires et d'éléments suspicieux additionnels. Ce dossier permet l'ajout d'alertes générées par le logiciel ou de signalements externes, lequel sera éventuellement envoyé à l'analyse de deuxième niveau. Si les transactions accumulées dans le dossier nécessitent d'être envoyées au CANAFE, la DOD sera plus rigoureuse, étant donné que plusieurs éléments ont été accumulés dans le dossier.

Dans le cas où l'alerte n'est pas fermée, c'est-à-dire que la transaction est douteuse, celle-ci se rend au deuxième niveau d'analyse, soit une analyse approfondie effectuée par des analystes plus expérimentés. Le traitement d'une alerte à ce niveau est d'approximativement 3h et les analystes vont par conséquent, analyser moins d'alertes quotidiennement que les analystes de premier niveau. Des recherches plus élaborées doivent être faites à ce niveau ainsi que la rédaction de rapports d'analyse. De plus, le traitement peut être plus long selon les recherches et demandes qui doivent être faites. À

cet égard, diverses recherches peuvent être effectuées par les analystes : appels téléphoniques aux clients et demandes en succursales. Toutefois, l'appel de clients ne se fait pas systématiquement, dans un cas de figure où un individu considéré à risque et ayant des antécédents judiciaires, l'appel ne serait pas effectué, étant donné que le client, criminalisé, ne collaborerait pas avec la banque. Dans cette situation, une DOD serait envoyée directement au CANAFE, sans recherches supplémentaires, de même pour toutes les transactions où un doute de blanchiment d'argent est présent. Lorsqu'une DOD doit être remplie et envoyée, un gestionnaire va en premier lieu approuver la rédaction d'une DOD. En deuxième lieu, l'analyste va remplir la DOD, qui sera revalidée par le gestionnaire, puis envoyée au CANAFE, en troisième lieu.

Ainsi, un filtrage est fait par le premier niveau qui envoie les cas qui nécessitent plus d'analyse au deuxième niveau. Il appert important de spécifier, que bien que les transactions soient surveillées par la banque, le système financier n'est pas ralenti et les clients ne sont pas impactés par ces analyses. À cet égard, le délai est d'environ 8h pour analyser les transactions par le logiciel. La banque procède à ces analyses après que la transaction soit effectuée et interviendra plus tard le cas échéant ; l'alerte ne bloque pas la transaction.

Cette transformation au sein des pratiques apportait un changement en terme de culture, mais également un changement par rapport à la façon de penser et d'analyser. En effet, lorsque la surveillance alors manuelle visait presque exclusivement les clients à risque, elle portait alors sur une clientèle pour laquelle il y avait déjà fort probablement du blanchiment d'argent ou un fort soupçon en la matière. De ce fait, les analyses étaient plus portées vers la DOD, étant donné que le doute était plus important : encore une fois, ces personnes étaient des clients à haut risque. Avec la surveillance automatisée de tous les membres, les alertes générées ne portent plus uniquement sur les clients à risque. Par conséquent, les analystes ne doivent plus considérer toutes les transactions comme nécessairement suspectes et doivent plutôt tenter de démontrer le contraire, soit prouver qu'il n'y a pas d'indicateurs de blanchiment d'argent et tenter de légitimer le comportement détecté. Ainsi, des DOD ne sont pas remplies pour toutes les alertes générées, puisqu'elles ne portent pas forcément sur des transactions réellement suspectes. En parallèle, avec

l'implantation de ce logiciel, les DOD envoyées au CANAFE sont donc considérées comme plus rigoureuses.

3.2. Les enjeux de l'appropriation de la technologie

Dans le cadre de l'appropriation de la technologie par les utilisateurs, certains enjeux ont émergé. D'une part, des enjeux techniques persistent suite à l'implantation du logiciel, en dépit des ajustements faits à ce dernier. En effet, les cartes de crédit ne sont pas traitées actuellement. Par conséquent, s'il y a un achat par le biais d'une carte de crédit, cette transaction ne sera pas immédiatement prise en considération ; celle-ci va être analysée lorsque le paiement de la carte de crédit va être fait, soit au moment du remboursement par un compte débit. Il s'agit d'un enjeu temporaire qui éventuellement sera résolu, lorsque le logiciel aura la capacité de surveiller les cartes de crédit en temps réel. Parallèlement, le logiciel de détection algorithmique et d'autres modules dépendent d'un module, lequel comporte certaines erreurs. De ce fait, des impacts se font ressentir sur tous les modules dépendants. Il s'agit donc d'enjeux d'ordre technique qui seront ultérieurement résolus lors de perfectionnement et d'ajustement du logiciel.

Bien qu'il s'agisse d'un système automatisé de surveillance, certains clients de la banque sont encore suivis manuellement. Actuellement, le logiciel ne détecte pas certains types de transactions qui ont fait l'objet de DOD par le passé. L'outil n'est donc pas encore assez peaufiné pour qu'une alerte soit automatiquement générée pour ces transactions. Il y a donc encore une surveillance transactionnelle manuelle :

> « Un des enjeux qu'on a rencontré c'est qu'on, on a évolué sur ce qu'on détectait avec [le logiciel] versus ce qu'on a déclaré dans le passé comme types de transactions pour les clients plus à risque. Puis on s'est rendu compte que c'était pas les mêmes transactions du tout, puis que probablement si on se fiait juste sur l'outil en tant que tel, on captait pas les transactions qu'on a déclaré dans le passé. Il fallait garder le suivi un peu plus manuel si on voulait... pour s'assurer que ces transactions-là sont encore filtrées jusqu'au jour où est-ce qu'on va pouvoir faire confiance à 100 % à notre outil. » (Entrevue 6).

Certains écueils au niveau technologique sont donc encore présents suite à l'implantation de l'instrument algorithmique.

D’autre part, des enjeux se situent au niveau de l’adaptation au nouvel instrument pour les utilisateurs. Effectivement, le logiciel implanté avait un impact énorme au sein des pratiques. Bien que les analystes provenaient de la banque et connaissaient d’autres modules, ceux-ci devaient se familiariser avec le nouveau module. En effet, alors qu’avant la surveillance transactionnelle était effectuée manuellement par des analystes, cette surveillance est maintenant faite par des algorithmes. De plus, la surveillance portait uniquement sur les individus à risque, alors que désormais ce sont tous les clients qui sont surveillés. Il y a donc un volume plus important de membres à surveiller. De surcroît, lorsqu’une transaction était suspecte, des recherches étaient effectuées, alors qu’avec le logiciel algorithmique, les transactions à analyser ne sont pas nécessairement suspectes. Ainsi, il s’agit de changements en terme de culture au sein de la banque, de transférer d’un traitement manuel à une surveillance automatisée.

En parallèle, l’espace physique où se trouvent les analystes présente un enjeu. En effet, les analystes travaillent dans un espace ouvert au sein duquel se trouve un mur central. De ce fait, la moitié des analystes sont face au gestionnaire et l’autre moitié sont situés de l’autre côté du mur. Ces analystes sont donc plus isolés, ils sont moins en contact avec le gestionnaire et risquent de se sentir à l’écart. Il s’agit d’une réelle préoccupation que les analystes ont fait ressortir en atelier.

Somme toute, l’implantation d’un nouvel outil de détection algorithmique a été motivée par plusieurs motifs, dont le principal était les exigences réglementaires. Afin de procéder à sa mise en œuvre, une préparation a dû être réalisée par la banque, et ce, en prévision des changements importants qui allaient se produire au sein des pratiques de la banque.

CHAPITRE 6 – DISCUSSION

L'objectif de la présente recherche était de combler certaines lacunes dans la littérature académique, au sein de laquelle des chercheurs se sont penchés, d'une part, sur la lutte contre « l'argent sale » et, d'autre part, sur l'usage des technologies de surveillance dans le domaine de la sécurité. En effet, plusieurs écrits portent sur la lutte au blanchiment d'argent et au financement du terrorisme et tout ce qui y a trait, que ce soit sur les enjeux législatifs et les pratiques soulevés, le rôle des différents acteurs sur les scènes nationale et internationale, etc. (Favarel-Garrigues, G., Godefroy T. et Lascoumes, P., 2009 ; Gilmore, 2011 ; Amicelle, 2013b ; Van Duyne, Harvey et Gelemerova, 2018 ; Stessens, 2000 ; Roberge, 2004 ; Levi, 2002). De même, l'utilisation des nouvelles technologies au sein des organisations de *policing* a été couverte par la littérature, mettant notamment en lumière les bienfaits espérés et les usages concrets (Byrne et Marx, 2011 ; Tanner et Meyer, 2015 ; Chan, 2001 ; Dupont, 2004). De plus, plusieurs auteurs se sont plus particulièrement intéressés au *Big Data* et aux algorithmes en matière de sécurité, soulevant par le fait même les enjeux et critiques en ce qui a trait à leur utilisation (Lyon, 2014, Ceyhan, 2006 ; Aradau et Blanke, 2015 ; Amoore, 2009 ; Pasquale, 2016 ; Kitchin, 2014b). Or, les écrits actuels ne mettent pas en relation ces deux littératures, c'est-à-dire qu'ils ne portent pas sur l'utilisation des nouvelles technologies de surveillance par les banques, dans une perspective de lutte au blanchiment d'argent et au financement du terrorisme. Ainsi, la recherche visait à combler ces lacunes et visait plus précisément à répondre à la question suivante : Dans quelles mesures les nouveaux instruments algorithmiques implantés au nom de la lutte au blanchiment d'argent et au financement du terrorisme font une différence en matière de surveillance au sein des banques canadiennes ?

L'étude de Le Bourhis et Lascoumes (2014) ainsi que l'étude d'Amicelle, Aradau et Jeandesboz (2015) ont été utilisées comme cadre théorique. Ces études ont été mobilisées afin de procéder à l'analyse des résultats de la présente recherche. Les trois espaces de résistance soulevés par Le Bourhis et Lascoumes (2014) ont été utilisés comme canevas, soit la conception de l'instrument, sa mise en œuvre ainsi que son appropriation par les utilisateurs. De plus, l'étude d'Amicelle, Aradau, et Jeandesboz (2015) a mis de l'avant la

possibilité d'effets inattendus lorsqu'un instrument de sécurité est en contact avec les utilisateurs et le contexte d'action spécifique. Ainsi, cette étude a été utilisée tout au long de l'analyse quant aux effets et enjeux soulevés lors du contact entre les utilisateurs avec l'instrument algorithmique et le contexte d'action de la banque.

Ainsi, la revue de la littérature, présentée précédemment, a illustré le rôle fondamental qu'occupent désormais les banques en ce qui a trait à la surveillance financière en matière de lutte au blanchiment d'argent et au financement du terrorisme (Favarel-Garrigues, Godefroy et Lascoumes, 2009). Effectivement, la surveillance des flux financiers vise à déceler des transactions réalisées à la suite d'un crime et des transactions effectuées dans le but d'éventuellement commettre un crime (Amicelle, 2013b). Ainsi, les banques sont désormais des « sentinelles de l'argent sale » et se retrouvent par conséquent avec de nouvelles obligations, notamment celles de devoir connaître leurs clients, de surveiller les transactions et de rapporter les transactions suspectes (Favarel-Garrigues, Godefroy et Lascoumes, 2009 ; Amicelle et Iafolla, 2017 ; Amicelle, 2008 ; de Goede, 2017b ; Amicelle, 2018). Les résultats de la recherche illustrent donc, d'une part, les nouvelles responsabilités imputées aux banques et, d'autre part, les actions mises en branle par les banques afin de satisfaire à ces responsabilités. De fait, alors qu'une exigence réglementaire exige désormais la banque à surveiller tous ses clients, celle-ci a procédé à l'implantation d'un outil algorithmique. À cet égard, « [l]'intégration d'instruments automatisés a eu un effet important sur l'organisation du travail interne des banques et la transformation des pratiques. » (Favarel-Garrigues, Godefroy et Lascoumes, 2009, p 201.).

Dans une logique de compréhension de l'espace de sélection et de mise en œuvre de l'instrument ainsi que de l'espace d'appropriation par les utilisateurs, la recherche tentait de saisir la façon dont l'instrument fait une différence dans les pratiques de l'organisation. En effet, « [t]enir compte des processus d'appropriation des nouvelles technologies est crucial pour être en mesure de (mieux) comprendre les pratiques de policing et de sécurité. » (Amicelle, 2019, p.19). Dans un premier temps, le nouvel instrument algorithmique implanté au nom de la lutte au blanchiment d'argent et au financement du terrorisme modifie la façon de surveiller les flux financiers. Effectivement, tel que présenté précédemment, l'instrument algorithmique permet de surveiller tous les clients de la

banque et plus uniquement ceux qui présentent un risque élevé. À cet égard, bien qu'une personne ne présente pas un risque élevé, celle-ci peut tout de même avoir un comportement transactionnel considéré comme suspect, d'où l'importance de surveiller tous les clients. De même, tel que mentionné dans la revue de la littérature, les instruments technologiques ont notamment permis aux organisations policières de procéder à des analyses plus avancées, telles que l'analyse des empreintes digitales, la lecture des plaques d'immatriculation, etc. (Ratcliffe, 2016 ; Byrne et Marx, 2011). Les analyses permises par les technologies apparaissent donc comme une plus-value pour ces organisations policières et pour la banque. Ainsi, dans le cadre de la recherche, l'instrument algorithmique implanté permet la surveillance de tous les clients, ce qui constitue un changement majeur en matière de surveillance pour la banque.

Dans un deuxième temps, l'outil introduit au sein des pratiques bancaires vise, grâce aux algorithmes, à détecter certains patterns, qui ne peuvent être détectés à l'œil nu. De plus, comme abordé dans la revue de la littérature et souligné par les participants, les banques doivent surveiller des milliers de transactions, ce qui rend la détection de transactions suspectes ardue (Roberge, 2004 ; Amicelle, 2019). Par conséquent et encore une fois, des outils technologiques sont ainsi utilisés afin de surveiller en continu les flux financiers (Amicelle, 2008). De surcroît, tel qu'abordé dans la revue de la littérature, les pratiques liées au *Big Data* ainsi que l'analyse prédictive visent à dévoiler des patterns inattendus et à repérer de potentielles « *needles in the haystack* » (Chan et Bennett Moses, 2017 ; Aradau et Blanke, 2015 ; Aradau et Blanke, 2017). Conséquemment, les algorithmes sont utilisés pour analyser ces masses de données, dont l'analyse dépasse la capacité humaine (Lyon, 2014 ; Chan et Bennett Moses, 2017). Pour ce faire, Amoore (2009) et les participants mentionnent qu'un calcul est effectué à partir de certains aspects, qui va générer une alerte lorsqu'un pointage est atteint. Toutefois, Chan et Bennett Moses (2017) mentionnent que dans une perspective de *Big Data*, peu importe la quantité de données disponibles, il ne s'agit jamais de données complètes. D'ailleurs, les participants ont souligné le manque de données notamment en raison des employés en succursales et de la perte d'informations lors de transferts d'un système à un autre. De plus, Chan et Bennett Moses (2017) mentionnent que la quantité massive de données peut « brouiller » les signaux, ce qui a été

soulevé par un participant, mais dans une différente optique. En effet, lors de la paramétrisation de l'instrument, la banque a décidé de ne pas sélectionner trop d'algorithmes afin d'éviter de perdre les transactions pertinentes dans un fort volume d'alertes. De surcroît, Lyon (2014) mentionne que dans une logique de « *finding the needle in the haystack* », il est possible qu'un volume important de faux positifs en découle, ce que les participants ont d'ailleurs corroboré, mentionnant qu'il y avait plus ou moins 90 % des alertes qui étaient des faux positifs. Somme toute, il est possible de constater qu'il s'agit d'un changement en matière de surveillance pour la banque, de posséder un logiciel qui permet d'analyser des données de masse d'une part, et qui permet, d'autre part, de détecter des patterns que l'humain ne pourrait détecter.

Ainsi, bien que l'outil algorithmique implanté produise des effets considérés comme positifs quant à l'analyse des flux financiers, certains problèmes techniques en découlent. De fait, tel que présenté dans la revue de la littérature, plusieurs problèmes et préoccupations découlent de l'utilisation de nouvelles technologies dans le cadre de la surveillance. Effectivement, Dupont (2004) souligne qu'il est possible que l'implantation de technologies engendre des problèmes, lesquels ne seront pas nécessairement réglés immédiatement. D'ailleurs, les résultats de la recherche ont mis en lumière un problème relatif à la qualité des données. D'une part, les codes de transactions regroupent divers types d'opérations financières qui diffèrent les uns des autres et, d'autre part, les employés des succursales n'entrent pas toujours les bons codes. Ce problème relatif à la qualité des données a notamment des impacts pour l'équipe antiblanchiment de la banque et celui-ci ne peut être réglé de façon imminente. De même, le problème relatif à la « segmentation » des populations, malgré les conséquences engendrées, ne peut être réglé immédiatement et requiert du temps et du travail. De plus, certains problèmes surviennent uniquement lorsque l'instrument technologique est en contact avec les utilisateurs (Amicelle, 2019 ; Dupont, 2004). En effet, le logiciel algorithmique et d'autres fonctionnalités du logiciel dépendent d'un module en particulier, lequel comprend des erreurs, et par conséquent impacte ceux dépendants. De surcroît, l'aspect technologique du logiciel peut éventuellement être problématique. De fait, les technologies requièrent des mises à jour et elles évoluent rapidement, rendant les dernières innovations plutôt désuètes (Tanner et Meyer, 2015 ;

Dupont, 2004 ; Ericson et Haggerty, 1997). D'ailleurs, tel que mentionné dans la revue de la littérature, certains policiers critiquent leur organisation de ne pas être capable de suivre l'évolution technologique (Tanner et Meyer, 2015). À cet effet, certains participants soulignent que bien que l'instrument choisi réponde actuellement aux besoins de la banque et qu'il soit à jour technologiquement, il est possible que dans quelques années l'instrument ne soit plus actuel.

Parallèlement à ces problèmes techniques, des préoccupations émergent également en ce qui a trait à l'utilisation de nouvelles technologies en matière de surveillance. En effet, bien que la revue de la littérature ait grandement soulevé un enjeu et une préoccupation à l'égard de la protection de la vie privée, cet aspect n'est pas ressorti dans la présente recherche. Malgré le fait qu'une grande partie de la littérature se soit penchée sur la surveillance et les algorithmes, il s'agit d'une littérature essentiellement théorique qui renvoie à des sources de secondes mains et qui est basée sur peu de données empiriques. Dans ce contexte, la présente recherche contribue aux débats en étant quant à elle basée sur des données empiriques ; un cas précis qui a permis de faire ressortir plusieurs problèmes concrets. De plus, la littérature met de l'avant la complexité des algorithmes (Bennett Moses et Chan, 2018). Toutefois, dans le cadre de cette recherche, il a été possible de constater que les algorithmes sont relativement simples, dans la mesure où il s'agit de comportements déterminés qui génèrent des alertes. Ainsi, malgré leur « simplicité », ces algorithmes engendrent plusieurs problèmes. Il n'en reste pas moins que malgré ces problèmes, un changement s'est produit au sein des pratiques et de l'organisation.

Dans un dernier temps, il convient d'insister sur le fait que l'instrument algorithmique implanté change de façon considérable les pratiques au sein de la banque, en ce qui a trait à la lutte au blanchiment d'argent et au financement du terrorisme. Tel que mentionné précédemment, Rogers (2003) précise que l'introduction d'une technologie peut engendrer des problèmes tout en présentant un changement majeur au sein des pratiques, nécessitant une période d'apprentissage. Effectivement, de nouvelles équipes ont dû être créées afin de travailler avec le logiciel, changeant la structure organisationnelle ; ce qui vient supporter ce que Favarel-Garrigues (2005b) et Favarel-Garrigues, Godefroy et Lascoumes (2009) mentionnent à l'égard de la réorganisation à laquelle les banques doivent procéder

afin de répondre aux exigences, c'est-à-dire de procéder à l'embauche de nouvelles personnes, de créer des formations et d'acquérir de nouvelles technologies. De plus, Tanner et Meyer (2015) soulignent que les nouveaux instruments technologiques nécessitent beaucoup de temps afin de comprendre leur fonctionnement. D'ailleurs, l'introduction de l'instrument algorithmique a nécessité beaucoup de temps en amont et en aval. En effet, la banque a eu recours à un accompagnement de transformation et à un « intégrateur de systèmes technologiques » afin de faciliter l'introduction, de créer des formations et de paramétrer l'outil. Les équipes ont ainsi dû apprendre de nouvelles pratiques de travail en ce qui a trait à l'utilisation du nouveau logiciel. De plus, la façon de traiter les alertes a changé, dans la mesure où lorsque seulement les clients à risque étaient surveillés, il y avait un fort soupçon, alors que maintenant tous les clients sont surveillés. De ce fait, les alertes ne portent plus nécessairement sur des personnes à risque et les transactions ne sont donc pas forcément suspectes. Par conséquent, les participants soulignent que les déclarations d'opérations douteuses (DOD) sont désormais plus rigoureuses à la suite de l'implantation, dans la mesure où les alertes générées sont analysées de manière approfondie. Ainsi, le fait qu'une équipe soit formée uniquement pour traiter les alertes générées par le logiciel algorithmique change et améliore, idéalement, la surveillance au sein de la banque.

Par ailleurs, au même titre que pour les organisations policières, les participants soulignent que l'implantation d'une nouvelle technologie au sein de la banque fut réalisée dans une optique d'efficacité, d'efficience ainsi que pour satisfaire aux nouvelles exigences (Chan, 2001 ; Ratcliffe, 2016). Bien qu'il soit possible que des personnes résistent à l'implantation d'un nouvel outil, dans le cadre de la recherche, les personnes ne se sont pas opposées à l'utilisation de cet outil (Chan, 2001 ; Éricson et Haggerty, 1997 ; Rogers, 2003). À cet effet, Chan (2001) souligne que l'implantation d'une nouvelle technologie au sein des pratiques peut mener au refus de l'utiliser. De plus, la structure organisationnelle peut résister à l'implantation de nouvelles technologies au sein des pratiques (Rogers, 2003 ; Ericson et Haggerty, 1997). Or, Ratcliffe (2016) mentionne que l'implantation de nouvelles technologies au sein des pratiques policières était plus acceptée si ces technologies permettaient d'améliorer les tâches traditionnelles plutôt que créer de nouvelles tâches. À cet égard, dans le cadre de cette recherche, les analystes étaient enclins à participer à ce

projet ; bien qu'il s'agisse de nouvelles tâches reliées à la surveillance de tous les clients, ces tâches font partie des obligations, récentes, mais non nouvelles, d'une banque en matière de lutte au blanchiment d'argent et au financement du terrorisme. Parallèlement, les personnes étaient enthousiastes et ne démontraient pas de résistance face au changement, car celui-ci n'était pas imposé aux analystes qui étaient volontaires pour être affectés à la nouvelle unité. En revanche, le changement était imposé à la banque et à l'équipe antiblanchiment dans son ensemble en raison des exigences réglementaires imposées. Toutefois, il y avait une capacité d'appropriation, c'est-à-dire qu'il était possible pour la banque de choisir l'outil et de le paramétrer selon ses besoins. Enfin, les outils technologiques sont souvent implantés afin d'améliorer l'efficacité de l'organisation, par contre, dans le cas des organisations policières, Dupont (2004) et Byrne et Marx (2011) mentionnent que leurs performances ne sont pas améliorées. Ainsi, bien que les participants mentionnent que les DOD sont maintenant plus rigoureuses à la suite de l'implantation de l'outil algorithmique, il est encore difficile et tôt pour savoir si l'outil améliore réellement les pratiques de la banque en matière de surveillance.

CONCLUSION

Les résultats de la recherche ont mis de l'avant les changements apportés par l'implantation d'un outil algorithmique au sein des pratiques de la banque en matière de surveillance, et ce, au nom de la lutte au blanchiment d'argent et au financement du terrorisme. Cet instrument a été implanté afin de satisfaire à une nouvelle exigence, soit celle de surveiller tous les clients de la banque. Bien qu'il ne s'agissait pas d'une exigence de recourir à un système automatisé, en raison du volume important de transactions financières, la banque a opté pour cette solution.

L'intérêt porté au blanchiment d'argent trouve racine aux États-Unis durant les années 1960 dans le cadre de la Guerre à la drogue et les années subséquentes (Gilmore, 2011). La lutte internationale au blanchiment d'argent a ensuite été déclenchée à la suite du Sommet du G7 en 1989, lors de la création du GAFI, structure intergouvernementale créée à cet effet (Gilmore, 2011 ; Favarel-Garrigues, Godefroy et Lascoumes, 2009). Enfin, la lutte au financement du terrorisme s'est jointe à la lutte au blanchiment d'argent, à la suite des évènements du 11 septembre 2001, évènements ayant intensifié l'attention portée au terrorisme (Banifatemi, 2002). De ce fait, les banques, de même que d'autres acteurs privés, tels que les avocats et notaires, se retrouvent avec de nouvelles responsabilités et doivent « *policer* » leurs clients (Svedberg Helgesson et Mörth, 2018 ; Amicelle, 2013b). En effet, les banques doivent surveiller les transactions financières et sont dorénavant considérées comme des « sentinelles de l'argent sale » (Favarel-Garrigues, Godefroy et Lascoumes, 2009). Conséquemment, plusieurs obligations leur sont incombées, dont celles de surveiller les transactions, de rapporter les transactions suspectes, de connaître leurs clients, etc. (Amicelle et Iafolla, 2017 ; Amicelle, 2008 ; de Goede, 2017b ; Amicelle, 2018). Pour ce faire, les banques doivent procéder à des restructurations au sein de leur organisation et notamment procéder à l'implantation de nouveaux outils technologiques (Favarel-Garrigues, 2005b ; Favarel-Garrigues, Godefroy et Lascoumes, 2009). Dans ce cadre, des outils d'analyse sont utilisés afin d'entre autres déceler des transactions suspectes et détecter des transactions effectuées par des personnes figurant sur des listes antiterroristes. (Amicelle, 2008 ; Ryder, 2012 ; Amicelle, 2019).

D'ailleurs, les pratiques en matière de surveillance ont évolué et ont été reconfigurées à l'ère numérique (Lyon, 2014). À cet égard, en 2013, les révélations d'Edward Snowden ont mis de l'avant les pratiques de surveillance des gouvernements et les pratiques liées au *Big Data* (Pasquale, 2016 ; Lyon, 2014). De ce fait, l'utilisation de données à des fins de sécurité est perçue à nouveau comme un problème politique en lien avec certaines libertés et droits fondamentaux (Bauman et al., 2015 ; Aradau et Blanke, 2015). Toutefois, pour les professionnels de la sécurité, le *Big Data* apparaît plutôt comme la solution aux problèmes contemporains de sécurité, dans l'optique où les algorithmes permettent de détecter des patterns au sein de ce volume (Aradau et Blanke, 2015 ; Aradau et Blanke, 2017 ; Lyon, 2014 ; Chan et Bennett Moses, 2017). D'ailleurs, les algorithmes sont utilisés à plusieurs finalités dans le domaine de la sécurité, notamment dans la gestion des listes antiterroristes, de la surveillance des flux financiers, au sein des pratiques policières et dans les aéroports (Amoore, 2009 ; Bennett Moses et Chan, 2018 ; Amicelle, 2019 ; Phillips et Pohl, 2018).

Ainsi, ces nouvelles technologies sont de prime abord implantées au sein des organisations afin d'être notamment plus efficaces, efficientes et pour répondre à de nouvelles exigences (Chan, 2001 ; Ratcliffe, 2016). Toutefois, il est possible que des problèmes découlent de l'implantation, dont certains étaient alors inconnus au moment de l'introduction (Chan 2001 ; Rogers, 2003). De plus, ces technologies apportent des changements majeurs au sein des pratiques de l'organisation (Sasidharan, 2015). Par conséquent, alors que certaines personnes peuvent être en faveur de l'implantation, il peut y avoir présence de résistances de la part d'autres personnes (Chan, 2001 ; Éricson et Haggerty, 1997 ; Rogers, 2003).

La littérature s'est donc intéressée d'un côté, à la lutte au blanchiment d'argent et au financement du terrorisme et d'un autre côté, aux nouvelles technologies dans le domaine de la sécurité ainsi qu'à leur implantation. Par contre, aucune recherche empirique ne s'est intéressée à l'utilisation de ces nouvelles technologies en matière de surveillance dans le cadre de la lutte au blanchiment d'argent et au financement du terrorisme par les banques. De ce fait, la présente recherche permet de combler ces lacunes dans la littérature. Plus particulièrement, la recherche s'est intéressée à l'implantation d'un outil algorithmique au sein d'une banque et visait éventuellement à répondre à la question suivante : Dans quelles mesures les nouveaux instruments algorithmiques implantés au nom de la lutte au

blanchiment d'argent et au financement du terrorisme font une différence en matière de surveillance au sein des banques canadiennes ?

La recherche visait à comprendre l'espace de sélection et de mise en œuvre de l'instrument ainsi que l'espace d'appropriation par les utilisateurs. Dans cette optique, les résultats ont mis de l'avant les différences en matière de surveillance à la suite de l'introduction de l'instrument algorithmique implanté au nom de la lutte au blanchiment d'argent et au financement du terrorisme. Dans un premier temps, l'outil modifie la façon de surveiller les flux financiers, dans la mesure où tous les clients de la banque sont désormais surveillés. Dans un deuxième temps, l'outil permet de détecter des patterns qui ne peuvent être détectés à l'œil nu et permet l'analyse de données de masse. Dans un dernier temps, l'instrument change fortement les pratiques au sein de la banque, où de nouvelles équipes ont dû être créées afin de travailler avec l'outil, de même que de nouvelles pratiques de travail. Bien que l'instrument algorithmique ait produit des changements majeurs au sein des pratiques en matière de surveillance, son efficacité reste à établir vu son caractère récent. Il pourrait donc être intéressant d'étudier les améliorations apportées quant aux pratiques de surveillance et notamment de déterminer si les DOD, perçues comme plus rigoureuses, mènent à davantage d'enquêtes, voire d'arrestations.

BIBLIOGRAPHIE

Amicelle, A. (2008). 9. La lutte contre le financement du terrorisme. Dans *Au nom du 11 septembre..: Les démocraties à l'épreuve de l'antiterrorisme*, Paris: La Découverte, 131-138.

Amicelle, A. et Favarel-Garrigues, G. (2009). La lutte contre l'argent sale au prisme des libertés fondamentales : quelles mobilisations ?, *Cultures & Conflits*, No. 76, pp. 39-66. http://journals.openedition.org/conflits/17768?gathStatIcon=true&lang=fr

Amicelle, A. (2011). Towards a 'new' political anatomy of financial surveillance. *Security Dialogue*, 42(2), 161-178. https://doi.org/10.1177/0967010611401472

Amicelle, A. (2013a). Gestion différentielle des illégalismes économiques et financiers ; Les questions fiscales dans l'anti-blanchiment. *Champ Pénal*, 10, 1-23, https://journals.openedition.org/champpenal/8403

Amicelle, A. (2013b). Les professionnels de la surveillance financière. Le malentendu comme condition de possibilité. *Criminologie*, 46 (2), 195-209.

Amicelle, A., Aradau, C. et Jeandesboz, J. (2015). Questioning security devices : Performativity, resistance, politics. *Security Dialogue*, 46(4), 293-306.

Amicelle, A. et Jacobsen K.U., E. (2016). The Cross-Colonization of Finance and Security through Lists: Banking Policing in the UK and India. *Environment and Planning D: Society and Space*, 34(1), 89-106.
http://journals.sagepub.com/doi/abs/10.1177/0263775815623276

Amicelle, A. (2017). When finance met security : Back to the War on Drugs and the problem of dirty money. *Finance and Society*, 3(2), 106-123, https://doi.org/10.2218/finsoc.v3i2.2572

Amicelle, A. et Iafolla, V. (2017). Reporting Suspicion in Canada : Insights from the fight against money laundering and terrorist financing. *Canadian network for research on terrorism, security and society*, 17(4).

Amicelle, A. (2018). Policing through misunderstanding : insights from the configuration of financial policing. *Crime Law Social Change*, 69(2), 207-226.

Amicelle, A. (2019, disponible sur demande). Policing et nouvelles technologies à l'ère numérique.

Amoore, L. (2009). Algorithmic War : Everyday Geographies of the War on Terror. *Antipode*, 41 (1), 49-69, https://doi.org/10.1111/j.1467-8330.2008.00655.x

Aradau, C. et Blanke, T. (2015). The (Big) Data-security assemblage : Knowledge and critique. *Big Data & Society*, 1-12. https://doi.org/10.1177/2053951715609066

Aradau, C. (2015). The signature of security : Big data, anticipation, surveillance. *Radical philosophy*, 191, 21-28.

Aradau C. et Blanke, T. (2017). Politics of prediction : Security and the time/space of governmentality in the age of big data. *European Journal of Social Theory*, 20(3), 373-391, https://doi.org/10.1177/1368431016667623

Bauman, Z., Bigo, D., Esteves, P., Guild, E., Jabri, V., Lyon, D. et Walker, R.B.J. (2015). Repenser l'impact de la surveillance après l'affaire Snowden : sécurité nationale, droits de l'homme, démocratie, subjectivité et obéissance. *Cultures & Conflits*, 98, http://journals.openedition.org/conflits/19033

Banifatemi, Y. (2002). La lutte contre le financement du terrorisme international. *Annuaire français de droit international*, 48, 103-128. http://www.persee.fr/doc/afdi_0066-3085_2002_num_48_1_3694

Bennett Moses, L. et Chan, J. (2018). Algorithmic prediction in policing : assumptions, evaluation, and accountability. *Policing and Society*, 28 (7), 806-822.

Bures, O. (2012). Private Actors in the Fight Against Terrorist Financing : Efficiency Versus Effectiveness. *Studies in Conflict & Terrorism*, 35(10), 712-732. https://doi.org/10.1080/1057610X.2012.712032

Byrne, J. et Marx, G. (2011). Technological Innovations in Crime Prevention and Policing - A Review of the Research in Implementation and Impact. *Journal of Police Studies, 3*(20), 17-40.

Canafe (2019). Qu'est-ce que le blanchiment d'argent ? Repéré à https://www.fintrac-canafe.gc.ca/fintrac-canafe/definitions/money-argent-fra

Cardon, D. (2015). *À quoi rêvent les algorithmes : Nos vies à l'heure des big data*. Paris, France : Le Seuil.

Cameron, I. (2003). European Union Anti-Terrorist Blacklisting. *Human Rights Law Review*, 3 (2), 225-256.

Ceyhan, A. (2008). Technologization of Security : Management of Uncertainty and Risk in the Age of Biometrics. Surveillance & Society, 5(2), DOI: 10.24908/ss.v5i2.3430

Ceyhan, A. (2006). Enjeux d'identification et de surveillance à l'heure de la biométrie. Cultures & Conflits, 64, DOI : 10.4000/conflits.2176

Chan, J. (2001). The technological game : How information technology is transforming pratice. *Criminal Justice*, 1(2), 139-159, https://doi.org/10.1177/1466802501001002001

Chan, J. et Bennett Moses, L. (2017). Making Sense of Big Data for Security. *The British Journal of Criminologie*, 57 (2), 299-319.

Chappez, J. (2003). La lutte internationale contre le blanchiment des capitaux d'origine illicite et le financement du terrorisme. *Annuaire français de droit international*, 49, 542-562, https://doi.org/10.3406/afdi.2003.3765.

de Goede, M. (2011). Blacklisting and the ban: contesting targeted sanctions in Europe. *Security Dialogue*, 42(6), 499-515. DOI: 10.1177/0967010611425368.

de Goede, M. et Sullivan, G. (2016). The politics of security lists. *Environment and Planning D : Society and Space*, 34 (1), 67-88.

de Goede, M. (2017a). Banks in Frontline : Assembling Space/Time in Financial Warfare. Dans Christopher, B., Leyshon, A. et Mann G. (eds.), *Money and Finance After the Crisis : Critical Thinking of Uncertain Times*. New Jersey, États-Unis : John Wiley & Sons Ltd.

de Goede, M. (2017b). The chain of security. *Review of International Studies*, 44 (1), 24-42.

de Goede, M. (2018). Counter-Terrorism Financing : Assemblages After 9/11. Dans King, C. (eds.), Walker, C. (eds.) et Gurulé, J. (eds.), *The Palgrave Handbook of Criminal and Terrorism Financing Law*. Palgrave Macmillan, 755-779.

Dijck, J.V. (2014). Datafication, dataism and dataveillance : Big Data between scientific paradigm and ideology. *Surveillance & Society*, 12(2), 1477-7487.

Dupont, B. (2004). La technicisation du travail policier : ambivalences et contradictions internes. *Criminologie*, 37(1), 107-126, https://doi.org/10.7202/008719ar

Eason, K. (1988). *Information Technology and Organisational Change*. Taylor & Francis Group.

Eckert, S. (2008). The US regulatory approach to terrorist financing. Dans Biersteker, T.(eds.) et Eckert, S. (eds.), *Countering the financing of Terrorism*. New York : Routledge, 209-233.

Eckert, S., Biersteker, T.J. et Tourinho, M. (2016). Introduction. Dans Eckert, S. (eds.), Biersteker, T.J.(eds.) et Tourinho, M(eds.), *Targeted Sanctions : The Impacts and Effectiveness of United Nations Action*. United Kingdom : Cambridge University Press, 1-10.

Ericson, R.V., et Haggerty, K.D. (1997). *Policing the risk society*. Toronto, Canada :

University of Toronto Press.

Favarel-Garrigues, G. (2003). L'évolution de la lutte antiblanchiment depuis le 11 septembre 2001. *Critique internationale*, 20(3), 37-46, doi:10.3917/crii.020.0037.

Favarel-Garrigues, G. (2005a). La reformulation domestique russe des enjeux moraux de la lutte anti-blanchiment. *Revue internationale des sciences sociales*, 185(3), 573-584. doi:10.3917/riss.185.0573.

Favarel-Garrigues, G. (2005b). Le renouvellement des listes noires de la lutte contre l'argent sale. *Criminologie*, 38(2), 91-102, doi:10.7202/012663ar.

Favarel-Garrigues, G., Godefroy T. et Lascoumes, P. (2007). Les sentinelles bancaires de l'antiblanchiment : Acteurs privés et *policing* économique. *Sociologie du travail*, 49(1), 10-27.

Favarel-Garrigues, G., Godefroy T. et Lascoumes, P. (2009). *Les sentinelles de l'argent sale*. Paris, France : Les Éditions La Découverte.

Foumdjem, C. (2011). *Blanchiment de capitaux et fraude fiscale*. Paris, France : L'Harmattan.

GAFI. (s.d.). À propos du GAFI. Repéré à https://www.fatf-gafi.org/fr/aproposdugafi/

Gilmore, W. (1992). International efforts to combat money laundering. *Commonwealth Law Bulletin*, 18(3), 1129-1142, DOI: 10.1080/03050718.1992.9986212.

Gilmore, W. (2011). *Dirty money : The evolution of international measures to counter money laundering and the financing of terrorism* (4e édition). Strasbourg, France : Council of Europe.

Guild, E. (2008). The Uses and Abuses of Counter-Terrorism Policies in Europe : The Case of the 'Terrorist lists'. *Journal of Common Market Studies*, 46(10), 173-193, https://doi.org/10.1111/j.1468-5965.2007.00772.x

Hunault, M. (2017). Réglementation relative à la lutte contre le blanchiment des capitaux et au financement du terrorisme. Dans : Michel Hunault éd., *La Lutte contre la corruption, le blanchiment, la fraude fiscale*. Paris: Presses de Sciences Po.

Johnson, J. et Jensen, C. (2010). The Financing of Terrorism. *Journal of the Institute of Justice and International Studies*, 10, 103-116.

Kitchin, R. (2014a). Big Data, new epistemologies and paradigm shifts. *Big Data & Society*, 1-12, https://doi.org/10.1177/2053951714528481

Kitchin, R. (2014b). *The Data Revolution : Big Data, Open Data, Data Infrastructures and Their Consequences*. Los Angeles : Sage Publications Ltd.

Kyriakos-Saad, N, Esposito, G et Schwarz, N. (2012). The incestuous relationship between corruption and money laundering. *Revue internationale de droit pénal*, 83, 161-172, DOI 10.3917/ridp.831.0161.

Le Bourhis, J-P. et Lascoumes, P. (2014). En guise de conclusion/Les résistances aux instruments de gouvernement : Essai d'inventaire et typologie des pratiques. Dans Halpern, C. (eds.), Lascoumes, P. (eds.) et Le Galès, P. (eds), *L'instrumentation de l'action publique* (p. 493-520). Paris, France : Les Presses de Sciences Po.

Levi, M. et Reuter, P. (2006). Money Laundering. *Crime and Justice*, 34(1), 289-375.

Levi, M. (2002). Money Laundering and Its Regulation. *American Academy of Political and Social Science*, 582, 181-194.

Levi, M. (2010). Combating the Financing of Terrorism: A History and Assessment of the Control of 'Threat Finance', *The British Journal of Criminology*, 50 (4), 650-669. https://doi.org/10.1093/bjc/azq025

LexisNexis. (s.d.). Processus de conformité & vérifications listes Personnes Politiquement Exposées. Repéré à https://bis.lexisnexis.fr/glossaire/ppe

Lyon, D. (2014). Surveillance, Snowden, and Big Data : Capacities, consequences, critique. *Big Data & Society*, 1-13, https://doi.org/10.1177/2053951714541861

Marron, D. (2008). Money Talks, Money Walks : The War on Terrorist Financing in the West, *Policing: A Journal of Policy and Practice*, 2 (4), 441-451.

Nance, M.T. (2018a). The regime that FATF built : an introduction to the Financial Action Task Force. *Crime Law Social Change*, 69 (2), 109-129.

Nance, M.T. (2018b). Re-thinking FATF : an experimentalist interpretation of the Financial Action Task Force. *Crime Law Social Change*, 69 (2), 131-152.

Onderco, M. (2011). Managing the Terrorists : Terrorists Group Blacklisting in Beck's World. *Perspectives*, 19(1), 27-48. http://www.jstor.org/stable/23616170

Paillé, P. et Mucchielli, A. (2016). *L'analyse qualitative en sciences humaines et sociales* (4e ed.). France : Armand Colin.

Pasquale, F. (2016). Une nouvelle course aux armements : surveillance des données informatiques et finance dématérialisée. *Perspectives libres*, 177-196.

Phillips, P. J. et Pohl, G. (2018). Terrorism Watch Lists, Suspect Ranking and Decision-

Making Biases. *Studies in Conflict and Terrorism*, DOI: 10.1080/1057610X.2018.1432046

Pinson, G. et Sala Pala, V. (2007). Peut-on vraiment se passer de l'entretien en sociologie de l'action publique ? *Revue française de science politique*, 57 (5), 555-597.

Ratcliffe, J.H. (2016). *Intelligence-led Policing* (2e éd.). London : Routledge, Taylor & Francis Group.

Roberge, I. (2004). Le Canada et le régime international de lutte contre le blanchiment d'argent et le financement du terrorisme : Un exemple de coordination verticale et horizontale. *International Journal*, 59(3), 635-653.

Roberge, I. (2011). Dans Handbook of Transnational Governance : Institutions and Innovations. Financial Action Task Force. Edited by Thomas Hale and David Held.

Roach, K. (2011). *The 9/11 effect : Comparative counter-terrorism*. New York : Cambridge University Press.

Rogers, E.M. (2003). *Diffusion of innovations* (5e éd.). New York : Free Press.

Rouvroy, A. et Berns, T. (2013). Gouvernementalité algorithmique et perspectives d'émancipation : Le disparate comme condition d'individuation par la relation ? *Réseaux*, 177(1), 163-196, doi:10.3917/res.177.0163

Ryder, N. (2012). *Money Laundering – An Endless Cycle ? : A Comparative Analysis of the Anti-Money Laundering Policies in the United States of America, the United Kingdom, Australia and Canada*. New York : Routledge.

Sasidharan, S. (2015). Change Management, Knowledge Dynamics and Normative Influences in Entreprise Technology Implementation : An Empirical Study. *Asia-Pacific Journal of Management Research and Innovation*, 11(2), 81-94, DOI: 10.1177/2319510X15576274

Scherrer, A. (2006). La circulation des normes dans le domaine du blanchiment d'argent : le rôle du G7/8 dans la création d'un régime global. *Cultures et Conflits*, 62, 130-148, DOI : 10.4000/conflits.2069

Scura, K. (2013). Money Laundering. *American Criminal Law Review,* 50 (4)*,* 1270-1298.

Steinbock, D. J. (2006). Designating the Dangerous : From Blacklists to Watch Lists. *Seattle University Law Review*, 30, 65-118.

Stessens, G. (2000). *Money Laundering : A New International Law Enforcement Model*. Cambridge, United Kingdom : Cambridge University Press.

Svedberg Helgesson, K et Mörth, U. (2012). *Securitization, Accountability and Risk Management : Transforming the Public Security Domain*. New York : Routledge.

Svedberg Helgesson, K. et Mörth, U. (2018). Client privilege, compliance and the rule of law : Swedish lawyers and money laundering prevention. *Crime Law Social Change*, 69 (2), 227-248.

Tanner, S. et Meyer, M. (2015). Police work and new 'security devices' : A tale from the beat. *Security Dialogue*, 46(4), 384-400, DOI: 10.1177/0967010615584256

Thomas, S.L., Nafus, D. et Sherman, J. (2018). Algorithms as fetish : Faith and possibility in algorithmic work. *Big Data & Society*, 1-11, DOI:10.1177/2053951717751552

Van Den Herik, L. (2007). The Security Council's Targeted Sanctions Regimes : In Need of Better Protection of the Individual. *Leiden Journal of International Law*, 20(4), 797-807. Doi:10.1017/S0922156507004451

Van Duyne, P.C., Harvey, J.H. et Gelemerova, L.Y. (2018). *The Critical Handbook of Money Landering : Policy, Analysis and Myths*. London, United Kingdom : Palgrave Macmillan.

Waddington, P.A.J. (2008), '*Police culture'*, in T. Newburn and P. Neyroud (eds), Dictionary of Policing. Cullompton, Devon: Willan.

Weiss, R. S. (1994). *Learning from Strangers: The Art and Method of Qualitative Interview Studies*. New York: Free Press.