Surveillance et suspicion à l'ère numérique. Réflexions à partir de la politique mondiale contre l'argent sale

Anthony Amicelle, David Grondin

CHAMP PÉNAL
PENAL FIELD

Champ pénal/Penal field

31 | 2024
Le vingtième anniversaire de *Champ Pénal/Penal Field*

Surveillance et suspicion à l'ère numérique. Réflexions à partir de la politique mondiale contre l'argent sale

Surveillance and Suspicion in the Digital Age : Remarks in Light of the Global Policy against Dirty Money

Anthony Amicelle et David Grondin

OpenEdition Journals

Édition électronique
URL : https://journals.openedition.org/champpenal/15531
ISSN : 1777-5272

Éditeur
Association Champ pénal / Penal field

Ce document vous est fourni par INIST - Centre national de la recherche scientifique (CNRS)

cnrs

Référence électronique
Anthony Amicelle et David Grondin, « Surveillance et suspicion à l'ère numérique. Réflexions à partir de la politique mondiale contre l'argent sale », *Champ pénal/Penal field* [En ligne], 31 | 2024, mis en ligne le 29 août 2024, consulté le 06 septembre 2024. URL : http://journals.openedition.org/champpenal/15531

Ce document a été généré automatiquement le 6 septembre 2024.

Surveillance et suspicion à l'ère numérique. Réflexions à partir de la politique mondiale contre l'argent sale

Surveillance and Suspicion in the Digital Age : Remarks in Light of the Global Policy against Dirty Money

Anthony Amicelle et David Grondin

Introduction

1 La montée en puissance de l'intelligence artificielle et des algorithmes comme nouvelles figures du pouvoir de surveiller et d'agir à partir de vastes masses de données est devenu un enjeu incontournable en matière de contrôle social. Au cours des vingt dernières années, soit la période d'existence de *Champ Pénal*, ce sujet a en effet pris une importance considérable. Pourtant, il brille paradoxalement par son absence dans les publications de la revue. Ce numéro anniversaire constitue donc l'occasion idéale pour commencer à y remédier. Le présent article vise à poser un premier jalon en ce sens et, par-là même, à susciter d'autres contributions pour interroger plus avant la place de ces entités techniques dans le contrôle social au 21e siècle [1]. Et cette montée en puissance porte autant sur le *policing* des activités et marchés illicites que sur la régulation de celles et ceux qui sont formellement autorisés, soit deux facettes du contrôle social déjà amplement discutées en dehors de la revue.

2 Du côté du *policing*, l'importance prise par l'instrumentation algorithmique dans les politiques de sécurité apparaît comme une tendance lourde – certes contrastée mais transversale (Amoore, Raley, 2017 ; Egbert, Leese, 2021 ; Kaufmann, 2024) – dans les pays occidentaux et au-delà (Feldstein, 2019 ; McDaniel, Pease, 2021 ; Peeters, Schuilenburg, 2021). Elle se retrouve dans le quotidien de patrouilles de police

(Benbouzid, 2019) et de professionnels de la justice civile et pénale (Brayne, Christin, 2021 ; Dumoulin, 2022 ; Dubois, 2023 ; Girard-Chanudet, 2023), dans de nouvelles initiatives en matière de tranquillité urbaine (Castagnino, 2021), dans l'organisation d'événements sportifs tels que les Jeux Olympiques (Picaud, Adam, 2024), et dans le fonctionnement d'appareils nationaux et transnationaux de renseignement (Lyon, 2014 ; Chan, Bennett Moses, 2017 ; Bigo, Bonelli, 2019 ; Blackmore et al., 2022). À l'instar des « *machines prédictives* » en production et en service dans d'autres domaines d'activités (Benbouzid, Cardon, 2018), le graal des *big data* en matière de sécurité est souvent associé à la capacité prêtée aux systèmes algorithmiques de surveillance de créer un nouveau régime d'anticipation des événements (Aradau, Blanke, 2017 ; Christin, 2017 ; Kaufmann et al., 2019 ; Grondin, Hogue, 2023). Quoi qu'il en soit, la notion ambiguë de *big data* reste surtout utilisée pour signifier « le franchissement d'un seuil de quantité, de complexité, de rapidité de prolifération des données à partir duquel nous serions contraints d'automatiser et d'accélérer (pour tenir compte de l'accroissement continu, à grande vitesse, des masses de données) les processus de transformation des données numériques en informations opérationnelles » (Rouvroy, 2016 : 11). C'est notamment le cas pour traiter toujours plus rapidement de grandes masses de données commerciales, transactionnelles et communicationnelles relatives à des personnes et des choses en mouvement à des fins policières, judiciaires et de renseignement (de Goede, 2018). Dans ce cadre, l'expression de « systèmes algorithmiques » fait référence aux nouvelles technologies de traitement de données et aux techniques d'analyse prenant appui sur des *inputs* codés dans un format lisible pour une machine afin de générer des *outputs* sous une forme compréhensible pour des êtres humains (Bellanova *et al*. 2021, 129). En tant que modalité critique de surveillance dans une dynamique de « *policing* algorithmique » (Wessels, 2023), le rôle croissant de cette instrumentation et de ces interactions 'humain-machine' est ainsi abordé dans la littérature au regard de ses implications sur les pratiques de sécurité, sous l'angle de l'efficacité, des discriminations et de la gouvernance démocratique des politiques de lutte contre la criminalité et le terrorisme (Brayne, 2017 ; Ferguson, 2017 ; Shapiro, 2019 ; Lyon, Wood, 2021 ; Leese, 2024).

3 Du côté de la régulation, le concept de « régulation algorithmique » a fait florès au cours des dernières années dans la littérature anglophone, en particulier en matière de régulation économique et financière (Andrews *et al*., 2017 ; Yeung, 2017 ; Yeung, Lodge, 2019). Sa définition originelle renvoie à des « systèmes décisionnels qui régulent un domaine d'activité dans le but de gérer un risque ou altérer un comportement via la génération constante de connaissances par des modèles computationnels en collectant systématiquement (en temps réel sur une base continue) les données directement émises par de multiples composants dynamiques au sein d'un environnement régulé afin d'identifier et, si besoin, d'ajuster automatiquement les (ou susciter l'ajustement des) opérations du système pour atteindre un objectif prédéfini » (Yeung, 2017, 6). Le développement de tels systèmes algorithmiques vise à compléter si ce n'est à supplanter la supervision humaine pour directement orienter ou au moins informer la prise de décision en matière de régulation des comportements (Ulbricht, Yeung, 2022). L'émergence de cette forme de gouvernance algorithmique est présentée comme décisive pour la création d'environnements réglementaires « où tout écart aux normes et aux objectifs donnés puisse être détecté et corrigé comme jamais auparavant » (Bellanova, de Goede, 2022, 104). Et bien que la détection de déviances réglementaires puisse être effectuée de manière réactive, après leur occurrence, il y a

là aussi l'affirmation d'une ambition prédictive et préemptive sur la base de corrélations produites à partir de grandes masses de données (Yeung, 2017). De la même façon que pour le *policing* algorithmique, cette régulation par et à travers des algorithmes est analysée sous l'angle des justifications qui y sont apportées, de sa formalisation et de sa mise en œuvre concrète, de son efficience et de ses conséquences inattendues, et du degré de transparence et de responsabilité juridique qui en découle (Burk, 2019 ; Eyert *et al.,* 2022 ; Hildebrandt, 2018 ; Johns, Compton, 2022).

4 Le processus d'instrumentation algorithmique de la surveillance est donc un enjeu prégnant en matière de contrôle social, tant du côté du *policing* que de la régulation. Or, en tant que configuration originale entre *policing* et de régulation, l'action publique contre l'argent sale n'échappe pas à ce processus, bien au contraire, puisqu'il tend à y être particulièrement avancé. Le déploiement de systèmes algorithmiques de plus en plus sophistiqués s'est notamment banalisé en quelques années au sein du secteur bancaire, au gré des efforts renouvelés de vigilance à l'encontre des flux financiers illicites (Favarel-Garrigues *et al*., 2009 ; Han *et al.,* 2020 ; Singh, Lin, 2021 ; Lokanan, 2024). Et cette surveillance par algorithmes à des fins de *policing* a ouvert la voie à une surveillance de ces algorithmes et de leurs usages à des fins de régulation à l'occasion des contrôles de conformité anti-blanchiment auxquels sont soumises les banques (Amicelle, 2021). La conformité de ces institutions financières est de plus en plus scrutée et évaluée à l'aune de leurs équipements *high-tech*, et des utilisations qui en sont faites pour « suivre l'argent » - *Follow the money* selon le slogan officiel de la politique mondiale contre les flux financiers illicite - aux fins de prévention et de répression des crimes et désordres. Dans le cadre de cette politique, les institutions financières, à commencer par les banques, se trouvent ainsi en première ligne dans l'exercice d'une forme de *policing* algorithmique tout en étant les premières cibles d'une forme de régulation algorithmique. Dans le même temps, les instruments de surveillance algorithmique apparaissent quant à eux comme les nouveaux actants incontournables de cette double dynamique de contrôle social à l'ère numérique.

5 Malgré l'importance de tels développements dans le champ pénal en général et dans la lutte contre l'argent sale en particulier, les questionnements, les conséquences et les problèmes induits par le choix et l'utilisation croissante de cette instrumentation algorithmique sont encore mal cernés. C'est l'enjeu du présent texte que de s'y pencher en revenant sur un terrain de recherche effectué au Canada entre 2015 et 2019 (Amicelle, 2021), avant tout par entretiens au sein d'un échantillon représentatif de banques – principalement auprès des responsables de conformité anti-blanchiment et leurs équipes – et du service fédéral de renseignement financier, Canafe - Centre d'analyse des opérations et déclarations financières du Canada/*Fintrac - Financial Transactions and Reports Analysis Centre of Canada*[2]. Nous commençons par resituer ce terrain et cette recherche dans le cadre plus large de la surveillance et du contrôle des mobilités contemporaines. Il s'agit ensuite d'aborder les considérations théoriques relatives à l'analyse des algorithmes dans ce cadre, avant de présenter et discuter plus avant notre étude de cas sur l'essor des « machines soupçonnantes » dans les banques pour la production d'alertes de blanchiment d'argent et de financement du terrorisme.

1. Mobilités sous surveillance algorithmique

> Le concept de mobilités englobe aussi bien les mouvements de personnes, de capitaux et d'information à grande échelle sur toute la planète que des processus plus locaux comme les transports quotidiens, les mouvements dans l'espace public et les déplacements d'objets matériels au jour le jour. [...] Dans le secteur public comme dans le privé, les logiques de gouvernance et de protection de la responsabilité sont de plus en plus dictées par les appréhensions liées aux mobilités illicites et aux risques sécuritaires afférents. (Kevin Hannam, Mimi Sheller, and John Urry, "*Mobilities, Immobilities and Moorings*")

6 La question des mobilités est régulièrement posée en termes de sécurité ou plus exactement d'insécurité, en étant ramenée à des problèmes publics de crimes et désordres, avec les 'nouvelles technologies' brandies comme principale solution pour y répondre (Kotef, 2015 ; Leese, Wittendorp, 2017 ; Nolte, 2022). Il s'agirait de gérer ainsi la « tension dynamique entre liberté de mobilité et offre de sécurité » (Amoore *et al.*, 2008), ou encore ce qui est présenté comme un dilemme : comment faciliter les mouvements de personnes, de capitaux et d'informations tout en faisant respecter la législation contre les mobilités illicites ? Dans la littérature anglophone (Hein-Kircher, Distler, 2022), l'expression de *mobility/security nexus* est utilisée pour caractériser l'imbrication croissante des enjeux de sécurité et de mobilité dans le cadre d'un régime de gouvernance par lequel les différentes formes de mobilités sont censées être surveillées, contrôlée et *in fine* 'sécurisées' en recourant à des innovations technologiques dans le domaine du numérique et des *big data* (Grondin, 2020). Et alors que les régimes de mobilité des personnes, des capitaux et des données sont souvent différenciés sur le plan analytique, ils apparaissent étroitement liés dans les discours et pratiques sécuritaires. À titre d'exemple, ce n'est pas un hasard si les programmes de sécurité dotés de capacités de *dataveillance*[1], comme le programme étatsunien de traque du financement du terrorisme (Amicelle, 2014 ; de Goede, Wesseling, 2017 ; Davis, 2022) – sont officiellement mis en avant pour leur capacité à tirer profit de ces mobilités interconnectées. Les représentants du département du Trésor américain et la Commission européenne ont ainsi affirmé au fil des années que :

> « Les informations obtenues grâce au *TFTP* [*Terrorist Finance Tracking Programme*] peuvent servir à obtenir des indices permettant d'identifier et de localiser des personnes impliquées dans des réseaux terroristes, et à fournir des preuves d'activités de financement d'attentats terroristes. Par exemple, il est possible de localiser un suspect en vérifiant le moment et le lieu où il a fermé et/ou ouvert un nouveau compte bancaire dans une ville ou un pays autre que son dernier lieu de résidence connu. Cela indique clairement que la personne peut avoir déménagé. Toutefois, même lorsqu'un suspect ne change pas de compte bancaire mais se déplace en continuant d'utiliser l'"ancien' compte (notamment par des services bancaires en ligne), il a été possible de détecter le changement de lieu en vérifiant, par exemple, les paiements de certains biens ou services (travaux de réparation ou d'entretien, ou autres activités ayant habituellement lieu là où une personne réside). [...] Le programme de traque du financement du terrorisme peut être en mesure de fournir des informations essentielles sur les mouvements de terroristes présumés et sur la nature de leurs dépenses » (Commission européenne, 2006, 6).

7 Dans ce contexte, la mise en relation des différentes formes de mobilités aux fins de surveillance est explicite. Partant des données numériques liées aux transactions financières, ce programme de sécurité pourrait retracer les mouvements d'argent électroniques pour pister les personnes suspectées de terrorisme (de Goede, Westermeier, 2022). En d'autres termes, il s'appuie sur la production et la circulation de données numériques liées aux mobilités financières pour (re)trouver et suivre à la trace des mobilités humaines[2].

8 Dans cet article, il s'agit plus particulièrement de s'intéresser à la lutte contre l'argent sale afin de comprendre comment, par la surveillance de données numériques transactionnelles, une forme de *policing* est exercée par le biais d'infrastructures algorithmiques. À ce titre, et en résonnance avec l'usage de la métaphore de l'aiguille dans la botte de foin dans les discours contemporains sur le renseignement et la sécurité nationale (Aradau, 2015 ; Grondin, 2016), les fournisseurs commerciaux de systèmes technologiques de surveillance décrivent la détection d'argent sale comme « la recherche ultime de l'aiguille dans la botte de foin » (Conroy, 2015). Mais à qui incombe la tâche de trouver l'aiguille représentée par l'argent sale dans la botte de foin que constitue le système financier ? Dans le cadre du processus général de pluralisation de l'activité policière (Huysmans, 2014 ; Bowling *et al.*, 2019 ; Jobard, de Maillard, 2024), suivre l'argent pour faire la police ne repose pas seulement ni premièrement sur l'institution policière, mais sur un cercle sans cesse élargi d'institutions économiques et financières (Amicelle, Iafolla, 2018).

9 Au Canada, plus de 30 000 entreprises – du secteur bancaire à celui de l'immobilier – doivent se conformer à la législation nationale contre l'argent sale, elle-même issue de la politique mondiale en la matière, officiellement appliquée dans plus de deux cent pays et territoires. Leurs représentants doivent s'acquitter du 'devoir de vigilance' inhérent à cette politique, avec l'obligation de dénoncer certaines transactions financières à l'autorité étatique compétente, à savoir Canafe. Dans son rôle de « cellule de renseignement financier » (Amicelle, 2019), type d'institution existant officiellement dans 177 pays en 2024, « Canafe reçoit les déclarations des institutions financières et des intermédiaires, analyse et évalue les informations déclarées et communique les soupçons de blanchiment d'argent ou d'activités de financement du terrorisme aux autorités policières et à d'autres personnes dans la mesure où la Loi le permet. Canafe communique également au SCRS [Service Canadien du Renseignement de Sécurité] les informations relatives aux menaces pesant sur la sécurité du Canada » (Canafe, 2019a). Les agents de Canafe reçoivent chaque année plus de 500 000 déclarations d'opérations douteuses (Canafe, 2023), communément appelées « déclarations de soupçon » (Favarel-Garrigues *et al.*, 2009), essentiellement de la part des banques, principales sources de dénonciation en la matière avec 80% de l'ensemble des signalements effectués (Canafe, 2019b).

10 Dans l'optique de s'acquitter de leurs responsabilités légales, l'écrasante majorité des acteurs bancaires disposent d'infrastructures algorithmiques pour surveiller les flux financiers, et y détecter les activités suspectes en tentant de s'y retrouver dans l'avalanche quotidienne de données numériques générées par les transactions de leurs millions de clients. En prêtant attention au travail invisible ou à tout le moins invisibilisé de ces infrastructures autour du *nexus* sécurité/mobilité, notre objectif est de mettre en lumière l'impact d'une telle gouvernance par les algorithmes et la *big dataveillance* (Degli Esposti, 2014 ; Lyon, 2022). Nous cherchons à montrer en quoi cela

modifie les pratiques antérieures, et en particulier comment de tels dispositifs sociotechniques sont devenus partie intégrante des politiques en place. Pour ce faire, nous abordons les pratiques de surveillance financière à travers le type d'instrumentation algorithmique qui en est devenu la pièce maîtresse, contribuant par-là même à matérialiser et à opérationnaliser au quotidien l'action publique internationale contre l'argent sale.

2. Les algorithmes : médias logistiques de la *big dataveillance*

11 « Les médias logistiques – en tant que technologies, infrastructures et logiciels – coordonnent, capturent et contrôlent les mouvements des personnes, des ressources financières et des objets. L'infrastructure crée des mondes. La logistique les gouverne » (Rossiter, 2016, 4-5). Cette citation, qui résume assez bien la manière dont Ned Rossiter approche la théorie des infrastructures à partir des médias logistiques, suggère comment la réflexion sur les algorithmes et le *nexus* sécurité/mobilité met au premier plan cette question des infrastructures (Nolte, Westermeier, 2020 ; Weber *et al.*, 2017 ; Larkin, 2013 ; Hecht, 2011 ; Star, 1999). Pour comprendre ce *nexus* sécurité/mobilité, il tenir compte de la manière dont les infrastructures 'agissent' en arrière-plan – ce qu'elles 'font' quand elles fonctionnent en étant appropriées dans des contextes d'action spécifiques (Amicelle *et al.*, 2015). Selon Keller Easterling, les infrastructures *font* bel et bien quelque chose : elles rendent « certaines choses possibles et d'autres impossibles » (Easterling, 2014, 14). Pour saisir comment les mobilités des personnes, des capitaux, des données ou des objets se voient surveillées et contrôlées voire gouvernées dans ce cadre, il faut porter une attention particulière à la 'force d'action' de ces infrastructures, et en particulier aux algorithmes au sein et/ou en tant qu'infrastructures numériques.

12 « L'infrastructure se définit par le mouvement ou la structuration de la forme sociale. C'est la médiation vivante de ce qui organise la vie : le monde de la vie de la structure » (Berlant, 2016, 39). Cela fait écho à l'approche de Susan Leigh Star, qui considère « l'infrastructure [comme] un concept fondamentalement relationnel, qui ne devient infrastructure réelle qu'en relation avec des pratiques organisées » (Star, 1999, 388). Comme le souligne John Durham Peters, ce sont les infrastructures qui définissent les conditions des opérations : « Le travail des médias logistiques est d'organiser et d'orienter, de disposer les personnes et les biens, souvent sous forme de grilles. Ils coordonnent et subordonnent à la fois, en organisant des relations parmi les personnes et les choses » (Durham Peters, 2015, 37). Les algorithmes, entendus comme médias logistiques régissant les mobilités, agissent comme des infrastructures qui contribuent de plus en plus à organiser certaines sphères de la vie sociale. On conçoit dès lors toute l'importance d'une compréhension fine des mécanismes de gouvernance par les algorithmes. À ce titre, selon Rob Kitchin :

> « On ne saurait dissocier les algorithmes des conditions de leur développement et de leur déploiement [...] Par conséquent, les algorithmes ne peuvent être compris que comme relationnels, contingents, contextuels par nature, inscrits dans le contexte plus large de leur assemblage sociotechnique. De ce point de vue, « l'algorithme » n'est qu'une composante d'un dispositif de grande ampleur, ce qui signifie qu'il ne peut jamais s'entendre comme une forme de savoir ou un mode de fonctionnement technique, objectif et impartial » (Kitchin, 2016, 18).

13 Dans cette perspective, Louise Amoore et Rita Raley conçoivent l'algorithme « à la fois comme un processus technique et une synecdoque pour des assemblages sociotechniques toujours plus complexes et opaques » (Amoore, Raley, 2016, 1). Il est censé permettre à ses utilisateurs d'obtenir un résultat spécifique en utilisant sa capacité de calcul pour passer au crible de grandes quantités de données et accomplir des tâches dont les agents humains ne pourraient *a priori* pas s'acquitter dans les délais impartis (Cardon, 2016). Plus révélateur encore, les algorithmes sont devenus des artefacts « hypermédiatisés », omniprésents au quotidien, mus par une logique « intégrée à la trame même de tous les processus sociaux, de toutes ces interactions, toutes ces expériences dont le déploiement s'articule de plus en plus à l'informatique » (Roberge, Seyfert, 2016, 1), même si cela ne garantit en rien qu'ils puissent bien interpréter et comprendre le monde (Broussard, 2019).

14 En explorant sous cet angle l'articulation sécurité/mobilité, il s'agit de se donner les moyens d'analyser, dans une perspective infrastructurelle (Glouftsios, 2019 ; Grondin, 2020 ; Dijstelbloem, 2021 ; Westermeier, 2022 ; Narita, 2023), les questions de surveillance à l'ère numérique. Composante à part entière d'une infrastructure de contrôle social, les algorithmes 'travaillent' en arrière-plan, un peu comme dans la « société de la boîte noire » /*Black Box Society* décrite par Frank Pasquale (2015) pour évoquer les algorithmes associés aux mécanismes de contrôle des capitaux et de l'information, pesant ainsi sur des décisions prises à partir de l'hypothèse fausse d'une neutralité et d'une objectivité purement technique de ces algorithmes[1]. Chez Pasquale, la « boîte noire » est à la fois ce dispositif d'enregistrement servant au contrôle des données techniques dans l'industrie des transports (automobiles, avions et trains) et une métaphore qui évoque l'obscurité et l'opacité de systèmes complexes dont les rouages restent difficiles à déchiffrer et/ou à dévoiler. Penser le rôle algorithmes en matière de *big dataveillance*, c'est prendre en compte la façon dont les vastes flux de données numériques sur la vie, le comportement et la mobilité des personnes sont passés en revue et traités. Cela nécessite de saisir le travail de médiation des infrastructures – ce travail d'arrière-plan souvent invisible, que Lauren Bridges décrit comme « l'obscurcissement des infrastructures » (2021, 832). Adopter une telle perspective infrastructurelle permet de comprendre comment ce sont « des systèmes interconnectés de relations numériques, sociales et politiques » (Narita, 2023, 297). Cela permet dans le même temps de voir ce qui est en train d'être construit comme avenues possibles, quelles capacités et propriétés se trouvent « intégrées » dans l'infrastructure, et de « révél[er] le[ur]s logiques et le[ur]s rationalités » (*ibid*., 299).

3. L'essor des machines soupçonnantes

15 Notre étude de cas sur la surveillance financière au Canada illustre l'importance des instruments algorithmiques dans les modes de *policing* contemporains qui, selon Jef Huysmans (2014, 91), combinent « communication du risque et pratiques de surveillance pour assembler technologiquement et faire circuler le soupçon ». Et à cet égard, plus que la notion de « machines prédictives » évoquée en introduction (Benbouzid, Cardon, 2018), celle de « machines soupçonnantes » apparaît plus pertinente pour rendre compte du rôle central joué par l'instrumentation dite 'high-tech' de surveillance et de détection d'activités suspectes. Les fournisseurs de telles machines vendent aux représentants des institutions financières ce qu'ils décrivent

comme des solutions de « surveillance transactionnelle » à grand renfort de messages publicitaires répétés pendant une décennie comme celui-ci :

> « La solution *Actimize Suspicious Activity Monitoring* (SAM) associe une technologie de pointe à des années d'expertise humaine en matière de lutte contre le blanchiment d'argent, ce qui contribue à garantir une détection précise des alertes, une productivité accrue des équipes et une réduction des coûts des programmes de conformité. L'automatisation de la lutte contre le blanchiment d'argent combine l'IA, l'apprentissage automatique et l'automatisation des processus robotisés ; la solution permet une couverture de bout en bout pour la détection, la notation, l'alerte, le traitement et la déclaration des activités suspectes. Ainsi, les services de lutte contre le blanchiment d'argent peuvent surveiller plus efficacement les activités suspectes, avoir la certitude de prioriser les bons problèmes et les bons risques, et automatiser les processus tout en gardant la main sur la décision finale » (NICE Actimize, 2024a).

16 Avant d'observer les algorithmes en action et ce qui en résulte, au-delà des communications promotionnelles, commençons par une brève description de notre étude de cas.

3.1. L'exemple canadien

17 Pour rappel, d'un côté il y a donc officiellement 31 000 « entités déclarantes » – banques, fournisseurs d'assurance-vie, négociants en pierres précieuses, courtiers et promoteurs immobiliers, comptables, casinos, courtiers en valeurs mobilières, etc. Leurs représentants doivent faire en sorte que ces entreprises soient 'en règle'. Les dirigeants bancaires sont particulièrement sensibles au fait que leurs établissements soient reconnus comme étant en pleine conformité avec leur devoir de vigilance et de dénonciation de tout soupçon d'argent sale. Néanmoins, étant à la tête d'organisations à but lucratif spécialisées dans la prestation de services financiers, ils entendent aussi et surtout demeurer rentables et réaliser davantage de profits. De l'autre côté se trouve Canafe, dont les agents dépendent du travail de surveillance fait au nom et au sein de ces entités déclarantes qui ne sont pas des sociétés de sécurité privée, mais dont il est attendu qu'elles soient les yeux et les oreilles de l'État sécuritaire dans l'espace financier. Comme l'a résumé un porte-parole de la cellule de renseignement financier, « les déclarations qui nous sont faites sont absolument essentielles. Sans ces déclarations, Canafe peut fermer boutique. » (Bronskill, 2016).

18 Dans ce cadre, les acteurs bancaires doivent déclarer à Canafe à la fois les opérations jugées suspectes mais aussi toute une série d'autres transactions en fonction de critères dits objectifs, selon des seuils monétaires principalement. À l'aune des directives officiellement en vigueur au moment de notre recherche, sont considérées comme suspectes les opérations dont les entités déclarantes ont « des motifs raisonnables de soupçonner » qu'elles sont en lien avec la perpétration, ou une tentative de perpétration, d'une infraction de blanchiment d'argent ou de financement d'activités terroristes. Ces « 'motifs raisonnables de soupçonner' sont fonction de ce qui est considéré comme raisonnable dans votre situation, compte tenu des pratiques et systèmes commerciaux normaux dans votre secteur d'activité. Bien que la loi et son règlement d'application ne vous obligent pas spécifiquement à mettre en place un système automatisé de détection des transactions suspectes, vous pourriez décider qu'un tel système serait bénéfique pour votre entreprise » (Canafe, 2017).

19 Si la dernière phrase laisse à penser que le choix d'acquérir un système algorithmique de surveillance relève d'une démarche volontaire, l'ensemble des agents de Canafe rencontrés ont dépeint une réalité différente. Comme l'a résumé l'un d'eux : « Ils n'ont pas le choix. Écoutez, toutes les grandes banques que je connais, elles ont un système informatique pour ça » (Entretien avec un agent de Canafe, Canada, 2015). L'interprétation du cadre juridique s'inscrit dans un contexte de pratique qui pousse fortement les acteurs bancaires à sauter le pas et à s'équiper de machines soupçonnantes. Plus précisément, les représentants de l'autorité de régulation exigent que les entités régulées soient conformes au devoir de vigilance, tout en admettant qu'une petite agence immobilière n'a pas besoin - ni les moyens - de l'infrastructure attendue dans les plus grandes banques du pays pour identifier les clients, enregistrer et conserver les données transactionnelles, surveiller les comportements et les flux financiers et, *in fine*, dénoncer les activités suspectes. Confrontés au déluge journalier de données numériques liées aux transactions bancaires – plusieurs millions d'opérations quotidiennes pour chacune des 6 principales institutions financières du Canada – les représentants de ces institutions financières se sont résolus à mettre en place des 'solutions technologiques' pour être estampillées conformes (Amicelle, 2021). Par conséquent, la nature a priori non-contraignante de la référence formelle aux systèmes de surveillance automatisés est devenue, en pratique, une obligation catégorique, particulièrement pour les banques, au Canada comme à l'international: « Les régulateurs font pression sur les petites institutions financières pour qu'elles adoptent des solutions plus automatisées, tout en poussant les grandes institutions financières à raffiner davantage encore leurs solutions actuelles » (Conroy, 2015).

20 Cette évolution n'a pas été sans créer des tensions au sein du secteur bancaire, et ce à deux niveaux principaux: (1) autour de l'articulation des principes hétéronomes de *policing* – retraduits en coûts de conformité réglementaire – avec les objectifs bancaires d'accumulation du capital ; et (2) autour des difficultés relatives à l'implantation et au fonctionnement concret des machines soupçonnantes. Comme pour toute infrastructure informationnelle, gérer ces tensions requiert de « rendre visible une infrastructure qui, dans d'autres contextes, est devenue invisible » *et* de lui conférer du sens ainsi qu'une utilité pour des « usagers radicalement différents » (Flichy, 2013). Répondre à ces exigences est une gageure tant pour les chercheurs en sciences sociales que pour les professionnels de la finance et de la sécurité, avec pour ces derniers nombre d'incompréhension et de problèmes inhérents à la mise en œuvre de la *big dataveillance* financière. En analysant la manière dont la « logistique » détermine pour partie la « pratique », on peut voir en quoi les algorithmes, en tant que médias logistiques, font partie intégrante de formes contemporaines de gouvernance, y compris en matière de contrôle social. C'est en déplaçant le regard analytique sur la façon ou plutôt les façons dont est « fait appel » à des dispositifs sociotechniques, dont ils sont mis à contribution, dont ils sont « sollicités » pour finalement être intégrés aux infrastructures autour du *nexus* sécurité/mobilité, qu'il devient possible de rendre compte des « choix humains et institutionnels [ainsi que la science, les rationalités et les technologies] qui se cachent derrière ces mécanismes froids » (Gillespie, 2014).

3.2. Conformité défendable et fardeau financier

21 Que ce soit avec des dirigeants réticents ou affichant la meilleure volonté du monde en matière de lutte contre l'argent du crime et du terrorisme, une banque reste encore

une fois une entreprise à but lucratif dans le domaine des services financiers. Concilier ces deux dimensions, et les velléités potentiellement contradictoires qui peuvent y être associées, a des conséquences sur l'instrumentation de la surveillance et ses usages. D'un côté, comme déjà amplement démontrée dans la littérature académique, au fil du temps les représentants des banques sont devenus sensibles au risque réputationnel associé aux questions d'argent sale (Gelemerova, 2009 ; Amicelle, 2011 ; Favarel *et al.*, 2011 ; Ball *et al.*, 2015). « Protégez votre réputation » demeure le principal slogan et un des arguments de vente majeurs des technologies de surveillance financière. À titre d'exemple, le slogan de la société américaine *NICE Actimize* – firme dominante dans ce marché porteur avec des clients parmi les banques canadiennes et d'autres tels que Barclays, la Société Générale et UBS – est le suivant : « Restez protégé. Préservez la conformité. Notre mission : lutter contre la criminalité financière ». La présentation de ses « solutions anti-blanchiment » lie capacité d'action contre des activités de criminelles et respect des obligations réglementaires : « Leader du marché dans les domaines du crime financier, du risque et de la conformité, NICE Actimize dispose d'une grande expertise dans ces domaines ainsi que d'une compréhension globale des menaces auxquelles votre organisation doit faire face. À partir d'une approche holistique et à l'aide de technologies novatrices et flexibles, nous vous aidons à détecter et à prévenir toute fraude potentielle. Vous êtes ainsi en mesure de gérer la conformité réglementaire et d'identifier les tentatives de blanchiment d'argent rapidement et avec précision. Vous protégez ainsi votre institution des crimes financiers, prévenez les risques réglementaires et les dommages réputationnels » (NICE Actimize, 2024b). Comme nombre de ses concurrents, fournisseurs auto-proclamés de protection institutionnelle, juridique et réputationnelle, son produit phare est un instrument de surveillance transactionnelle, connu sous l'acronyme S.A.M. pour *Suspicious Activity Monitoring*. La promesse est de « surveiller et détecter constamment les activités suspectes. Nous vous offrons une surveillance des transactions AML [*Anti-Money Laundering*] intelligente destinée à vous protéger des programmes de blanchiment d'argent inconnus » (*ibid.*). Ce discours est redoublé au sein des banques par ceux dont la conformité avec la politique contre l'argent sale est leur raison d'être :

> « Je pense que la motivation pour se conformer c'est, vous savez, de protéger l'image de marque de la banque. Et on veut que les clients et les actionnaires aient le sentiment d'une banque sûre, où ils peuvent effectuer des transactions sans avoir à s'inquiéter. Cette banque sera-t-elle ouverte demain ? Y a-t-il des problèmes liés aux personnes à qui elle prête de l'argent ? A-t-elle de bonnes pratiques commerciales ? La conformité nous permet de donner ce type de confiance à nos clients, ainsi qu'à nos employés en interne et aussi à nos actionnaires. Nous considérons cela comme une proposition de valeur, alors qu'auparavant la conformité était considérée comme un coût de fonctionnement ou une dépense. Aujourd'hui, nous considérons la conformité comme notre capacité à contribuer à l'image de marque, à la sûreté et à la solidité de l'organisation. Nous pensons qu'il s'agit d'un avantage concurrentiel » (Entretien avec un responsable de la conformité d'une banque, Canada, 2016).

22 Outre ces éléments de justification, l'accent mis sur les éventuelles amendes et sanctions administratives et pénales encourues pour non-conformité vient en complément de l'argument de vente que constitue la protection de la réputation. Les responsables de la conformité anti-blanchiment mentionnent également la crainte du retrait total ou partiel de la licence bancaire, ainsi que la possibilité de pertes financières consécutives à la réaction négative des autres banques – certes

concurrentes mais aussi partenaires commerciaux essentiels en matière de correspondance bancaire – en cas de sanction pour non-respect du devoir de vigilance en général, et des obligations de surveillance et de dénonciation en particulier. En effet, au-delà d'éventuelles retombées du côté de la clientèle, peu démontrées (Harvey, Lau, 2009), ces sanctions pour non-conformité ont un impact important sur la réputation d'un établissement et sur sa cote de risque au sein du champ (trans)national qu'est le 'secteur bancaire'. Tout établissement ainsi pris en défaut sera considéré à risque élevé par les autres, avec des conséquences majeures pour le maintien et le développement de relations d'affaires interbancaires.

23 Cette réfraction des principes hétéronomes de lutte contre l'argent sale sous forme d'exigences de conformité, principes qui deviennent dès lors partie intégrante de l'activité bancaire, signifie que ces exigences sont appréhendées au pire comme un fardeau réglementaire inévitable et au mieux comme un avantage concurrentiel. Néanmoins, le paradoxe de cette réfraction est que la principale préoccupation au sein des institutions financières est davantage lié à la non-conformité en tant que telle plutôt qu'à l'éventualité d'argent sale. Dans ce cadre, et bien que considérée indispensable pour faire état d'une « conformité défendable » (Ericson, 2007 ; Favarel-Garrigues *et al*., 2009), l'instrumentation de surveillance algorithmique reste perçue par les dirigeants bancaires comme un investissement coûteux, qui ne saurait offrir un retour adéquat pour des entreprises dont le cœur d'activité n'est pas la lutte contre la criminalité, les atteintes à l'ordre public et les menaces à la sécurité nationale. Dans ce contexte, une distinction est fréquemment invoquée dans le 'secteur bancaire', celle entre économiser ou ne pas perdre de l'argent/*saving money* (en évitant les sanctions pour non-conformité et les atteintes à la réputation) et gagner de l'argent/*making money* (*business as usual*) pour qualifier et clarifier le degré d'investissements à consentir :

> « Il y a encore …hum … quelques réticences sur les coûts. Il y a forcément une perte nette quelque part, on vous oblige à faire X, Y et Z… maintenant ils sont obligés d'adapter leur système informatique, leur technologie interne pour se mettre en conformité … Et ils disent : 'Vous savez, on ne peut pas se permettre tous ces changements technologiques juste comme ça, on a une entreprise à faire tourner. Vous [le régulateur/législateur] n'êtes pas le centre du monde.' Bref, c'est toujours une question d'argent et le moment n'est jamais bien choisi pour ça. Et ils disent : 'Maintenant ce n'est pas possible, on verra dans un an.' Sauf qu'il s'en passe des choses en un an, on est d'accord ? Donc, ils renâclent, mais leur service informatique renâcle aussi, dans l'autre sens, parce que la priorité c'est toujours de faire de l'argent. Mettons par exemple qu'ils doivent mettre en place un système informatique pour encaisser les frais de service. Ce système sera probablement prioritaire par rapport à ce qu'on leur demande, parce que ça touche le bilan comptable. Nous, on leur coûte de l'argent, on ne leur rapporte rien. Alors oui, on peut sauver leur réputation ! Sauf qu'ils [les dirigeants bancaires] ne voient pas les choses ainsi, mais alors pas du tout, jamais. Et c'est toujours… ce n'est pas juste les banques, c'est tout le monde [toutes les entités déclarantes]. Tout le monde renâcle à cause de l'aspect finance, du fardeau financier. Un fardeau, voilà ce que c'est pour eux [la lutte contre l'argent sale] : un fardeau financier » (Entretien avec un agent de Canafe, Canada, 2015).

24 Fortement ressentie dans les départements de conformité, cette pression à la rentabilité explique aussi la diversité constatée au sein du secteur bancaire en matière d'instrumentation de surveillance. Le niveau d'investissement et donc d'engagement technologique et, en conséquence, le degré de sophistication et de complexité des

opérations de surveillance reste en effet variable d'un établissement à l'autre, allant du strict minimum à une conception maximaliste des systèmes de surveillance algorithmiques.

4. Une distribution inégale des « solutions technologiques »

4.1. La version *high-tech* minimaliste

25 Au moment de notre enquête, certaines institutions financières n'avaient pas encore pleinement déployé d'instruments de surveillance algorithmiques aux fins de détection et de dénonciation d'activités et de transactions suspectes. L'investissement technologique a d'abord porté sur des systèmes automatisés plus simples, pour se conformer aux obligations déclaratives relatives à des seuils monétaires et à des listes nominatives plutôt qu'aux déclarations de soupçon.

26 Pour les opérations financières à déclarer sur la base d'un seuil monétaire, des instruments algorithmiques spécifiques ont par exemple été achetés et déployés pour repérer automatiquement les virements transnationaux de capitaux d'un montant supérieur ou égal à 10 000$, c'est-à-dire détecter « la réception d'instructions, par voie électronique, magnétique ou optique, ou au moyen d'un appareil téléphonique ou d'un ordinateur, pour le transfert d'une somme de 10 000 $ ou plus vers le Canada, ou vers l'étranger, en une seule; ou plusieurs opérations totalisant 10 000 $ ou plus au cours d'une même période de 24 heures effectuées par une même personne ou entité. » (Canafe, 2024b). En 2023, Canafe a reçu plus de 27 millions de déclarations relatives à ce type de transactions (Canafe, 2023).

27 Pour les opérations financières qui doivent être déclarées sur la base de régimes de sanctions nationaux ou internationaux, comme ceux du Conseil de sécurité des Nations Unies contre Al-Qaïda et Daech, la priorité a été donnée à la création de listes numériques consolidées de personnes et d'entités ciblées en utilisant des instruments de filtrage automatisés censés être capables de comparer ces listes nominatives avec les bases de données clients des banques pour identifier d'éventuelles correspondances ou relations financières pertinentes. Les acteurs bancaires doivent notamment soumettre des « rapports sur les biens terroristes » lorsqu'ils savent ou pensent que des actifs financiers sont liés à un groupe considéré comme terroriste ou à une personne connue et répertorié pour ses liens avec des entités listées[1]. Les pratiques de surveillance et de filtrage en la matière, avec ou sans technologies spécifiques, consistent également à compiler des revues de presse et à effectuer une veille en sources ouvertes.

28 Enfin, en ce qui concerne les opérations 'suspectes', les institutions financières qui, au moment de notre enquête, ne disposaient pas encore de systèmes algorithmiques de surveillance pleinement opérationnels, s'étaient engagés formellement dans cette voie, mais avec l'idée sans répétée par leurs représentants que cela prend du temps, à l'image de ce responsable conformité :

> « Au départ, il nous a fallu trois ans juste pour mettre au point la collecte de données, passer en revue le système bancaire, les données et déterminer… et je sais que nous ne sommes pas les seuls à avoir eu ce problème… bref, déterminer où se trouvaient toutes les données, comment les mettre au bon format et être en mesure d'identifier le type de transaction… Donc il y a énormément de manipulations en

> arrière-plan pour obtenir exactement les données dont on a besoin dans le système de surveillance transactionnelle, de manière à produire, au final, des alertes significatives » (Entretien avec un responsable de la conformité d'une banque, Canada, 2015).

29 Les agents de Canafe se sont faits à cette idée selon laquelle la surveillance et la détection algorithmique des activités suspectes impliquent un long processus de déploiement :

> « Deux ans, vous êtes bien optimiste ! Nous parlons de banques, elles ont des millions de clients, qu'il s'agisse de particuliers, d'entreprises, de grands groupes, et ainsi de suite. Et c'est encore pire quand on parle des grandes institutions financières. Le système informatique n'est pas seulement pour la banque mais pour toutes les filiales du groupe – assurance, assurance-vie, activités d'investissement et bien d'autres choses encore, au Canada et à l'étranger. Ainsi, le système commence souvent par la banque et s'étend progressivement aux autres filiales. La tâche est titanesque. C'est du très long terme. Et même quand c'est déployé, on est toujours en train de calibrer parce qu'il y a de nouveaux produits financiers, ou alors on a racheté un concurrent, ou on a oublié un marché, etc. » (Entretien avec un agent de Canafe, Canada, 2015).

30 Avant ou même pendant l'implantation d'une telle instrumentation algorithmique, le processus de production du soupçon d'argent sale exige beaucoup plus de travail manuel pour générer des alertes internes sur les opérations financières. Prenons l'exemple d'une banque avec 10 millions de clients. Avant le déploiement *high-tech*, la surveillance financière et la production des alertes afférentes se font en grande partie « à la main » pour reprendre l'expression des enquêtés, et ce principalement de deux façons, par une surveillance au guichet d'une part, et par une surveillance à distance indexée aux risques d'autre part (Amicelle, 2021). À cet égard, quand on examine le processus après déploiement d'un système algorithmique de surveillance des activités suspectes, on constate que la nouvelle infrastructure informationnelle change manifestement la donne.

4.2. La version *high-tech* maximaliste

31 Dans la version *high-tech* maximaliste d'un système de surveillance et de détection d'activités suspectes, les méthodes antérieures de vigilance perdurent. Néanmoins, le déploiement complémentaire d'une instrumentation algorithmique spécifique transforme à la fois la portée et la systématicité de la surveillance financière. En plus du filtrage basé sur les seuils monétaires et les listes consolidées issus des régimes (inter)nationaux de sanctions, toutes les transactions font désormais aussi l'objet d'une surveillance automatisée aux fins de détection d'activités suspectes. Il en résulte des alertes produites pendant la nuit, prêtes à être analysée le lendemain matin par des analystes regroupés à cet effet dans de nouvelles unités des départements conformité. Plus généralement, le système de surveillance et de détection des activités suspectes repose sur une combinaison de scénarios et/ou d'éléments analytiques. Les instruments algorithmiques, 'agissant' sous forme de machines soupçonnantes, sont basés sur une définition soit déductive soit inductive de l'anormalité, de l'inhabituel et, en fin de compte, du soupçon. En d'autres termes, la surveillance algorithmique aux fins de détection d'activité financière suspecte peut s'effectuer de deux façons.

32 Dans le premier cas de figure, les algorithmes de détection sont conçus pour repérer les transactions qui correspondent à un ensemble prédéfini de scénarios. Ces derniers –

également appelés règles – sont basés sur des indicateurs ou 'signaux faibles' provenant de sources internes et surtout externes aux banques, à commencer par ceux fournis par les agents de Canafe, et censés :

> « aider à évaluer si les transactions peuvent ou non donner lieu à des motifs raisonnables de soupçonner. Il s'agit par exemple d'indicateurs communs et spécifiques à un secteur d'activité qui peuvent être utiles lors de l'évaluation des opérations ou tentatives d'opérations. On y trouve des indicateurs basés sur certaines caractéristiques qui ont été liées au blanchiment de capitaux ou à des activités terroristes dans le passé. Ces indicateurs ont été collectés avec le concours des entités déclarantes, des organismes chargés de l'application de la loi et des unités internationales du renseignement financier » (Canafe/*Fintrac*, 2018).

33 Ces indicateurs officiels, près de 300, sont sélectionnés, combinés à d'autres, puis testés, (re)paramétrés voire supprimés plus ou moins régulièrement, soit par les fournisseurs de technologie, soit par des salariés de banque spécialisés sur le site d'utilisation :

> « Le groupe de triage [qui reçoit les alertes générées automatiquement] transmet en permanence des informations aux analystes [qui s'occupent du paramétrage des algorithmes sur site]. Ils leur disent : 'Vous savez, on a ceci ou cela qui revient tout le temps. Ce n'est rien, ce n'est rien. Pourrait-on optimiser les règles ?' C'est un processus continu, dans cet esprit, en vue d'optimiser les règles tout en construisant, grâce aux typologies et à d'autres éléments, de nouvelles règles pour introduire de nouvelles alertes. C'est un processus continu de maintenance et d'actualisation de nos règles » (Entretien avec un responsable de la conformité d'une banque, Canada, 2015).

34 Dans le second cas de figure, la surveillance financière dépend d'algorithmes conçus pour découvrir inductivement des « anomalies transactionnelles » et potentiellement suspectes, plutôt que par déduction à partir d'une comparaison avec un ensemble prédéfini de situations suspectes comme dans le cas précédent. Ce deuxième processus de production d'alertes repose sur le fait de constater qu'un client s'écarte du comportement transactionnel du groupe de pairs auquel il a été associé et/ou de son propre historique transactionnel individuel. Ce type d'alerte est donc le produit d'un double travail de catégorisation sociale – *social sorting* (Lyon, 2003), et de suivi dans le temps de l'activité transactionnelle. L'analyse de liens – *link analysis* – est également utilisée pour explorer les bases de données d'une banque afin d'identifier d'éventuelles associations qui pourraient être qualifiées de suspectes entre les clients (particuliers et entreprises), les comptes bancaires et les transactions (transferts de fonds électronique, dépôts d'espèce, etc.). Cette forme d'analyse de réseaux est souvent menée à partir des opérations ayant déjà généré une alerte, mais elle vise aussi de produire de nouveaux cas. Cela peut enfin être combiné à des instruments d'analyse automatisée de source de données non structurées telles que les sites web (veille médias, réseaux sociaux, etc.) ou les récits en « texte libre » contenus dans les déclarations de soupçon déjà transmises aux autorités par le passé.

35 En fin de compte, il va sans dire qu'il existe de grandes différences entre institutions financières, le long du continuum allant de la version minimaliste à la version maximaliste *high-tech* en matière de surveillance algorithmique. Malgré ces asymétries technologiques, tous les dirigeants de banques laissent leurs équipes de conformité se confronter au même enjeu : ne pas gêner l'accroissement des profits tout en évitant de se faire écraser entre le marteau d'une conformité défendable et l'enclume du fardeau financier d'un système d'alerte automatisé générateur de faux positifs en très grand nombre.

4.3. La gestion des faux positifs

36 « [Cinq] à 10% de toutes les alertes deviennent des cas significatifs. Il y a donc 90 à 95 % de faux positifs. Et ensuite, d'un cas significatif à une déclaration de soupçon, c'est moins de 10 %… moins de 10 % des cas significatifs se transforment en déclarations de soupçon » (Entretien avec un responsable de la conformité d'une banque, Canada, 2015). Selon ce responsable de conformité anti-blanchiment (dont les équipes disposent d'un système de surveillance proche de la version maximaliste), c'est au mieux une alerte sur 100 qui aboutit à une déclaration de soupçon de la part de son institution financière, ce qui se traduit tout de même chaque année par des milliers de déclarations de soupçon. Quelque soit la banque et le département de conformité, la tâche la plus fastidieuse reste le 'tri' des alertes – de quelques dizaines de milliers à plusieurs millions par an pour les plus grandes institutions financières – dont la plupart sont générées par les systèmes de surveillance algorithmiques. Un responsable de conformité soulignait ainsi le défi auquel sont confrontées tous ses homologues qui cherchent à réduire à la portion congrue le taux de « fausses alertes évidentes » :

> « C'est le problème le plus épineux, il y a beaucoup de faux positifs, et il y a toujours un équilibre à trouver entre dépenser de l'argent pour améliorer ce système et disposer de ressources suffisamment disponibles pour travailler là-dessus, ou bien passer en revue les faux positifs, et consacrer plutôt du temps là-dessus, donc c'est un problème et ce sera toujours un problème jusqu'à ce que je trouve quelqu'un qui me donne plus d'argent [rires]. Quoi qu'il en soit, les faux positifs resteront toujours présents, mais leur nombre doit être ramené à un niveau raisonnable pour qu'on ne reçoive des alertes que sur ce qui pose effectivement problème, et qu'on puisse couvrir l'activité sans avoir à filtrer tout ce 'bruit informationnel' autour – car une fois l'alerte générée, il faut l'examiner, c'est le minimum requis. Et à chaque fois, cela prend du temps » (Entretien avec un responsable de la conformité d'une banque, Canada, 2015).

37 L'étude des machines soupçonnantes et de la gestion des faux positifs permet de mieux comprendre comment les algorithmes 'agissent' en tant que médias logistiques de la surveillance financière. Pour paraphraser Evelyn Ruppert, les alertes ne surgissent pas de nulle part, elles résultent de multiples arrangements sociotechniques entre actants humains et non-humains (Ruppert, 2012). Comme pour d'autres pratiques contemporaines de *policing* et de sécurité, la capacité à produire des alertes émerge des relations – des connexions – entre un ensemble d'équipements et d'acteurs sociaux, depuis le concepteur de l'instrument de surveillance jusqu'à son utilisateur final. Si « l'action des utilisateurs est à la fois contrainte et rendue possible par les caractéristiques internes (techniques, logiques et cognitives) des instruments » (Amicelle *et al.*, 2015), il est essentiel de prêter attention aux caractéristiques variables des systèmes algorithmiques de surveillance et de détection d'activités suspectes afin de comprendre comment ils sont appropriés et mobilisés au quotidien. Plus précisément, dans le cas présent, comment les acteurs bancaires affinent-ils leurs pratiques de surveillance et de détection en fonction des caractéristiques spécifiques des 'solutions technologiques' qui sont les leurs ? La réponse à cette question repose en partie sur l'examen des relations qu'entretiennent ces acteurs avec les fournisseurs des 'solutions technologiques', relations qui peuvent aller d'une très forte dépendance à une relative autonomie. C'est aussi là que l'on peut voir et objectiver les relations de pouvoir à l'œuvre. Pour revenir à la métaphore de la boîte noire, la question cruciale

est alors de savoir qui – mais aussi comment et dans quelle mesure – est favorable à la préservation d'une boîte noire fermée à double tour plutôt qu'à son ouverture.

38 Les cas de dépendance élevée concernent les situations où l'instrumentation algorithmique reste à l'état de boîte noire pour les équipes de conformité, avec peu de marge de manœuvre. Les responsables et agents doivent s'en remettre à leur fournisseur pour tout changement, en particulier pour la modification et la création des algorithmes de détection :

> « Le problème, quand on touche aux algorithmes eux-mêmes, c'est qu'à chaque fois on fait appel au fournisseur, cela coûte de l'argent, et l'entreprise [sa banque, son employeur] n'est pas disposée à payer pour des suppléments… Or c'est ainsi que le modèle technique [des fournisseurs] est conçu. Il est conçu de telle sorte qu'une fois qu'ils deviennent votre fournisseur, ils commencent à vous facturer les prestations supplémentaires, parce qu'ils savent que vous n'avez nulle part où aller. Déployer un nouveau système informatique, ça coûte cher, surtout quand il faut faire une mise à niveau tous les deux ans parce que la technologie a progressé. Une fois qu'on a choisi un fournisseur, on le garde, sauf bouleversement inattendu » (Entretien avec un responsable de la conformité d'une banque, Canada, 2015).

39 À l'autre extrémité du continuum, par autonomie relative il faut entendre les situations où la capacité à mener des opérations d'ajustement, comme le paramétrage des règles existantes et la création d'algorithmes de détection supplémentaires, repose avant tout sur une expertise interne, en faisant appel à de nouvelles ressources humaines surnommées les « *data junkies* » :

> « C'est au niveau des analystes que nous développons les règles, les seuils, en fait c'est là que nous identifions les alertes qui pourraient constituer des cas d'opérations suspectes. Concrètement, ce sont eux qui programment les règles de surveillance des opérations, les algorithmes. Des statisticiens, des matheux qui développent les algorithmes pour les transactions, les sanctions, le rapprochement de données nominatives, tout… Mes analystes ont tous – pas tous mais la plupart – un master en *data science* ou un doctorat en *analytics*, c'est-à-dire qu'ils ont été biberonnés au monde de l'informatique ou aux méthodes quantitatives et computationnelles. Ils sont accros aux données – c'est pour ça qu'on les appelle *data junkies* – ils adorent les données, ils ne rêvent que de travailler avec les données » (Entretien avec un responsable de la conformité d'une banque, Canada, 2015).

40 Derniers venus dans le monde de la lutte contre l'argent sale à partir des années 2010, ces « *data junkies* » sont recrutés pour faire le lien avec les « *data-hungry beasts* » (monstres dévoreurs de données), tels que sont qualifiés en interne les systèmes algorithmiques, et affiner la surveillance en fonction des sessions de test, des retours internes et des nouveaux indicateurs disponibles. L'approche dite de la « boîte blanche » ou de l'« environnement ouvert [transparent] » est plus coûteuse que celle de la boîte noire algorithmique mais elle permet de mieux superviser tout ou partie du processus de surveillance en interne et ainsi d'être en mesure de mieux l'expliquer en retour au régulateur aux fins de conformité. *In fine*, l'argument de vente reste le même, « *saving money* », avec les mêmes formules commerciales du type : « Avez-vous réellement les moyens de recruter toujours plus de personnel pour gérer des volumes d'alertes en croissance continue ? ». Dans tous les cas, la réduction du nombre de faux positifs devient une fin en soi, loin devant l'objectif affiché de prévention et de répression des crimes et désordres par le suivi de l'argent.

Conclusion

41 La production dite automatisée de soupçons sous forme d'alertes se révèle moins automatisée que négociée, compte tenu des objectifs relativement distincts à faire tenir ensemble : faire toujours plus de profit, être conforme, contribuer à prévenir et réprimer les crimes et désordres.

42 *In fine*, la production algorithmique des alertes en matière d'argent sale diffère à bien des égards des mécanismes antérieurs toujours en place, et notamment dans le type de connaissances considérées comme pertinentes pour 'assembler' le soupçon. La forme et le contenu de ce qu'on sait des clients et de leurs transactions peuvent varier d'une banque à l'autre, d'un type de clientèle ou de relation d'affaires à l'autre, et d'un type d'employé de banque à l'autre (selon qu'il s'agit d'un conseiller en agence ou d'un analyste de données au siège). Dans ses travaux sur les technologies de surveillance et de contrôle, Clive Norris (2003) reprend la distinction opérée par John Dewey puis par Lyn Lofland entre la possibilité pour l'être humain de connaître une personne (une forme de familiarité appelée « *acquaintance-knowledge* ») ou de savoir des choses sur cette personne (« *knowledge-about* »). Il résume l'importance de cette distinction en matière de surveillance en notant que « la base, pour connaître les gens et non pas simplement savoir des choses sur eux, c'est l'interaction en face à face. Quand on ne connaît que des faits, le savoir dont on dispose n'est qu'indirect » (Norris, 2003, 251). Par définition, l'analyse et les analystes de données massives sont plus éloignés du contexte local que le personnel bancaire en succursale. La possibilité d'agir sur la base d'une familiarité procédant de l'interaction en face à face n'est dès lors plus une option. La surveillance algorithmique qui en découle, à distance et médiée par les *big data*, peut être considérée soit comme n'offrant que des connaissances extrêmement lacunaires, soit comme un facteur clé d'objectivité dans des activités de contrôle des mobilités – ici de capitaux.

43 La première interprétation souligne l'impossibilité avec l'instrumentation *de big dataveillance* de « comprendre en regardant quelqu'un si cette personne évite le contact visuel, si elle est très agitée ou pressante. Or ce sont des indicateurs qui montrent que quelque chose ne va pas » (Entretien avec un responsable de la conformité d'une banque, Canada, 2015). La seconde interprétation met en évidence le biais de connivence qui peut s'insinuer dans les interactions en face à face :

> « C'est souvent le cas, surtout quand les conseillers sont plutôt dans le relationnel avec la clientèle. Si vous prenez par exemple les activités de conseil en patrimoine, où le relationnel est au cœur même de l'activité, alors ils peuvent adopter un point de vue plus personnel, vous voyez – 'je connais le client, le client est bien, je le connais depuis dix ans, bla-bla-bla, normalement il n'y a rien à craindre'. Il faut donc toujours trouver un équilibre entre cet aspect et ce que l'on voit concrètement, sachant que parfois on tombe sur des choses qui nous rappellent durement à la réalité » *(ibid.)*.

44 Alors que ces deux interprétations sont ici formulées par le même responsable de conformité, elles illustrent plus généralement une tension classique en matière de surveillance et de contrôle des mobilités, avec un processus d'identification de cas suspects oscillant entre l'intuition humaine et le traitement automatisée des données massives. Dans la pratique, instinct et *big data analytics* sont souvent enchevêtrés, du paramétrage des instruments de surveillance algorithmiques jusqu'à l'envoi des déclarations de soupçon aux services répressifs de l'État.

45 Les algorithmes utilisés comme médias logistiques ont néanmoins des effets significatifs sur les opérations de surveillance. Leurs usages ont participé à normaliser une surveillance de masse, mais davantage aux fins de protection de la réputation des institutions bancaires que de lutte contre l'argent sale proprement dite, tout en étant source de déséquilibre par les nombreux faux positifs qui en découlent et qui doivent être analysées par des agents humains. Cela cristallise les tensions autour de la nécessité de concilier un problème présenté comme technique – à savoir le fonctionnement des machines soupçonnantes – avec une logique économique d'optimisation des coûts de ce fonctionnement. L'un des enjeux de cet article était de rendre davantage visible la complexité du processus de sélection et d'utilisation des algorithmes aux fins de *policing* et de régulation. Dans cette perspective, il s'agissait également de comprendre comment ce processus s'inscrit dans une articulation 'humain-machine', une infrastructure sociotechnique à laquelle l'algorithme est pleinement intégré. Déplacer le regard analytique sur les enjeux associés aux machines soupçonnantes permet de discerner à quel(s) endroit(s) les relations de pouvoir et les positions et prises de positions des uns et des autres sont déterminantes en matière de contrôle social. Ces machines à surveiller et à soupçonner sont donc installées au sein des principales entreprises du secteur financier afin de satisfaire aux exigences plus ou moins ajustées de régulation et de *policing*. Ainsi, tout en étant implantés dans les banques, ces actants désormais incontournables de l'action publique contre l'argent sale se retrouvent de fait aux frontières des champs de l'économie, de la régulation et de la sécurité. Leur omniprésence ouvre à cet égard de nombreuses pistes de recherche, dont deux principales sur lesquelles il convient de conclure cet article.

46 D'un côté, cette omniprésence, si elle reste appréhendée comme un centre de coûts dans le secteur bancaire comme dans d'autres sous-champs économiques, est devenu un business en soi et une source de profits pour de nouveaux agents économiques. En concurrence sur un marché international des technologies de surveillance et de conformité en perpétuel croissance, estimé à plus de 3 milliards de dollars en 2024, des entreprises privées font commerce de ces équipements, avec précisément une articulation des dimensions *policing* et régulation dans les discours de vente. Ce type de marché florissant reste encore à étudier, dans le sillage de quelques rares travaux pionniers sur les porteurs discrets de la surveillance financière (Favarel-Garrigues *et al.*, 2010).

47 De l'autre, la configuration de *policing* donnant corps à l'action publique contre l'argent sale n'est pas unique, avec de plus en plus d'équivalents dans d'autres politiques de sécurité. M. de Goede évoque à cet égard l'établissement de « chaînes de sécurité », « par lesquelles des données commerciales sont analysées, collectées, rapportées, partagées, déplacées et finalement déployées comme base d'intervention pour la police et à des fins de poursuite. Dans ce contexte, des compagnies privées – incluant Facebook et Twitter, des transporteurs aériens et des banques – se retrouvent en première ligne dans la lutte contre le terrorisme et d'autres menaces à la sécurité. Ces compagnies identifient, sélectionnent, recherchent et interprètent des transactions suspectes » (de Goede, 2018, 2). Qu'il s'agisse du cyberespace (Dupont, 2024), des grandes voies de circulation terrestres (Castagnino, 2017), maritimes (Nøkleberg, 2022), et aériennes (Glouftsios, Leese, 2023), ou encore une fois des circuits financiers, les politiques de sécurité et l'exercice du *policing* dépendent de plus en plus de ces compagnies, véritables piliers du capitalisme contemporain. Par-delà leurs différences,

ces organismes à but lucratif ont en commun d'être les opérateurs majeurs des mobilités transnationales, celles des personnes et des choses matérielles et immatérielles. Ils sont à l'œuvre dans « les grands lieux de la sécurité » que sont désormais tous les nœuds de communication et d'échange tels que les gares, les ports, les aéroports, les infrastructures routières, bancaires et les systèmes de paiement, ainsi que les plateformes de réseaux sociaux et de télécommunications (Gros *et al.*, 2008, 7 ; Gros, 2019). Ils permettent de connecter des zones géographiques sans pour autant être forcément situés aux confins des frontières physiques et souveraines des États et des ensembles régionaux. Engagés volontaires ou partenaires réticents, ils sont enrôlés pour surveiller ce qu'ils ont historiquement vocation à faire circuler, et ce afin d'enregistrer, repérer, signaler, tracer, filtrer voire bloquer les mouvements d'individus et de contenus suspects. L'exercice du *policing* a ainsi partie liée avec cette surveillance pratiquée par et au sein d'entreprises capitalistes de premier plan dont la logique économique est, de prime abord, relativement étrangère à celle du pénal et des interventions de sécurité. À ce titre, la place respective des systèmes de surveillance algorithmiques dans ces configurations de sécurité/mobilité gagnerait grandement à être interrogée dans une perspective comparée.

48 Amicelle A., 2011, Towards a 'New' Political Anatomy of Financial Surveillance, *Security Dialogue*, 42, 2, 161-178.

49 Amicelle A., 2014, (Il)légitimité du renseignement financierUsages transnationaux de la traçabilité des flux de capitaux, *Criminologie*, 47, 2, 77-104.

50 Amicelle A., 2019, Naissance d'une agence de renseignement : droits d'entrée dans les univers de la finance et de la sécurité, *Cultures & Conflits*, 114-115, 171-197.

51 Amicelle A., 2021, *Policing & Big Data*. La mise en algorithmes d'une politique internationale, *Critique internationale*, 3, 92, 23-48.

52 Amicelle A., Aradau C., Jeandesboz J., 2015, Questioning Security Devices: Performativity, Resistance, Politics, *Security Dialogue*, 46, 4, 293–306.

53 Amicelle A., Iafolla V., 2018, Suspicion-in-the-Making: Surveillance and Denunciation in Financial Policing, *British Journal of Criminology*, 58, 4, 845-863.

54 Amoore L., Raley R. (Eds.), 2017, Special Issue on Securing with Algorithms, *Security Dialogue*, 48, 1, p. 3-94.

55 Amoore L., Raley R., 2017, Securing with Algorithms: Knowledge, Decision, Sovereignty, *Security Dialogue*, 48, 1, 3-10.

56 Amoore L., Marmura S., Salter M. B., 2008, Smart Borders and Mobilities: Spaces, Zones, Enclosures, *Surveillance and Society*, 5, 2, 96-101.

57 Andrews L., Benbouzid B., Brice J., 2017, *Algorithmic regulation*, London, CARR, London School of Economics and Political Science Discussion Paper (85).

58 Aradau C., 2015, The Signature of Security: Big Data, Anticipation, Surveillance, *Radical Philosophy*, 191, 1-8.

59 Aradau C., 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.

60 Ball K.E., Dibb D.S., Canhoto A., Meadows M., Spiller K., 2015, *The Private Security State? Surveillance, Consumer Data and the War on Terror*, Frederiksberg, Copenhagen Business School Press.

61 Barocas S., Rosenblat A., Boyd D., Gangadharan S.P., Yu C., 2014, *Data & Civil Rights: Technology Primer*, Data & Society Research Institute.

62 Bellanova R., Irion K., Jacobsen K.L., 2021, Toward a Critique of Algorithmic Violence, *International Political Sociology*, 15, 121-150.

63 Bellanova R., de Goede M., 2022, The Algorithmic Regulation of Security: An Infrastructural Perspective, *Regulation & Governance*, 16, 1, 102-118.

64 Benbouzid B., 2019, To Predict and to Manage. Predictive Policing in the United States, *Big Data & Society*, 6, 1, 1-13.

65 Benbouzid B., Cardon D., 2018, Machine à prédire, *Réseaux*, 211, 5, 9-33.

66 Benjamin R., 2019, *Race After Technology: Abolitionist Tools for the New Jim Code*, Cambridge, Polity.

67 Berlant L., 2016, The Commons: Infrastructures for Troubling Times, *Environment and Planning D: Society and Space*, 34, 3, 393-419.

68 Bigo D., Bonelli L., 2019, Digital Data and the Transnational Intelligence Space, *in* Bigo D., Isin E., Ruppert E. (Eds.), *Data Politics: Worlds, Subjects, Rights*, London, Routledge, 100-122.

69 Blackmore, H., Chan J., Sanders C., Bennett Moses L., 2022, Datafication and the practice of intelligence production, *Big Data & Society*, 9, 1.

70 Brayne S., 2017, Big Data Surveillance: The Case of Policing, *American Sociological Review*, 82, 5, 977-1008.

71 Brayne A., Christin A., 2021, Technologies of Crime Prediction: The Reception of Algorithms in Policing and criminal courts, *Social Problems*, 68, 3, 608-624.

72 Bronskill J., 2016, Canadian Bank Fined $1.1M for Failing to Report Suspicious Transaction, Money Transfers, *The Star,* 5 April.

73 Broussard M. 2019, *Artificial Unintelligence: How Computers Misunderstand the World*, Boston, The MIT Press.

74 Burk D.L., 2019, Algorithmic Fair Use, *The University of Chicago Law Review*, 86, 2, 283-307.

75 Canafe, 2023, *Rapport annuel de CANAFE 2022-2023*, Ottawa, Canafe.

76 Canafe, 2019a, *Qu'est-ce que CANAFE ?,* Ottawa, Canafe.

77 Canafe, 2019b, *Rapport annuel de CANAFE 2018-2019*, Ottawa, Canafe.

78 Canafe, 2018, *Rapport annuel de CANAFE de 2017-2018*, Ottawa, Canafe.

79 Canafe/Fintrac, 2018, Financial Transactions that Must Be Reported, Ottawa, Canafe.

80 Canafe/Fintrac, 2017, *What is a Suspicious Transaction ?*, Ottawa, Canafe.

81 Cardon D., 2016, Deconstructing the Algorithm: Four Types of Digital Information Calculations, *in* Seyfert R., Roberge J. (Eds.), *Algorithmic Cultures: Essays on Meaning, Performance and New Technologies,* New York, Routledge, 95-10.

82 Cardon D., 2015, *À quoi rêvent les algorithmes ? Nos vies à l'heure des big data*, Paris, Le Seuil.

83 Castagnino F., 2021, *Les effets de l'intelligence artificielle sur l'activité policière : nouveaux régimes de quantification, diversification du marché et redéfinition des dispositifs de sécurité urbaine*, Paris, projet de recherche ANR.

84 Castagnino F., 2017, *Les chemins de faire de la surveillance : une sociologie des dispositifs de sécurité et de sûreté ferroviaires en France*, Thèse de doctorat, L'École des Ponts ParisTech.

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

86 Girard-Chanudet C., 2023, *La justice algorithmique en chantier. Sociologie du travail et des infrastructures de l'Intelligence Artificielle*, Thèse de doctorat, EHESS.

87 Christin A., 2017, Algorithms in Practice: Comparing Web Journalism and Criminal Justice, *Big Data & Society*, 4, 2, 1-14.

88 Clarke R., 1988, Information Technology and Dataveillance, *Communications of the ACM*, 31, 5, 498-512.

89 Commission Européenne, 2013, *Rapport conjoint de la Commission et du département du Trésor des États-Unis concernant la valeur des données fournies dans le cadre du TFTP*, Bruxelles.

90 Conroy J., 2015, *Global AML Vendor Evaluation*: *Managing Rapidly Escalating Risk*, Boston, Aite.

91 Davis J., 2022, Understanding the Effects and Impacts of Counter-Terrorist Financing Policy and Practice, *Terrorism and Political Violence*, 36, 1, 1-17.

92 Degli Esposti S., 2014, When Big Data Meets Dataveillance: the Hidden Side of Analytics, *Surveillance & Society*, 12, 2, 209-225.

93 de Goede M., 2018, The Chain of Security, *Review of International Studies*, 44, 1, 24-42.

94 de Goede M., Westermeier C., 2022, Infrastructural Geopolitics, *International Studies Quarterly*, 66, 3, 1-12.

95 de Goede M., Wesseling M., 2017, Secrecy and Security in Transatlantic Terrorism Finance Tracking, *Journal of European Integration*, 39, 3, 253-269.

96 Dijstelbloem H., 2021, *Borders as Infrastructure: The Technopolitics of Border Control*, Cambridge, Massachusetts, The MIT Press.

97 Dubois C., 2023, *Parler avec prudence des IA dans le droit et la justice*. https://orbi.uliege.be/bitstream/2268/308863/1/

98 Dumoulin L., 2022, *De quoi la 'justice prédictive' est-elle le nom ? Algorithmes, décision et jugement*, HDR, Université Paris-Saclay.

99 Dupont B., 2024, *La cybercriminalité. Approche écosystémique de l'espace numérique*, Paris, Armand Colin.

100 Easterling K., 2014, *Extrastatecraft: The Power of Infrastructure Space*, London, Verso.

101 Egbert S., Leese M. (Eds.), 2021, *Predictive Policing and Everyday Police Work*, New York, Routledge.

102 Ericson R., 2007, *Crime in an Insecure World*, London, Polity Press.

103 Eyert F., Irgmaier F., Ulbricht L. 2022, Extending the Framework of Algorithmic Regulation. The Uber Case, *Regulation & Governance*, 16, 1, 23-44.

104 Favarel-Garrigues G., Godefroy T., Lascoumes P., 2009, *Les sentinelles de l'argent sale : les banques aux prises avec l'antiblanchiment*, Paris, La Découverte.

105 Favarel-Garrigues G., Godefroy T., Lascoumes P., 2011, Reluctant Partners? Banks in the Fight against Money Laundering and Terrorism Financing in France, *Security Dialogue*, 42, 2, 179-196.

106 Favarel-Garrigues G., Godefroy T., Lascoumes P., 2010, Les porteurs discrets de la surveillance financière, *Critique internationale*, 3, 48, 77-95.

107 Feldstein S., 2019, *The Global Expansion of AI Surveillance*, Carnegie Endowment for International Peace, Working Paper.

108 Ferguson A.G., 2017, *The Rise of Big Data Policing*, New York, New York University Press.

109 Flichy P., 2013, Rendre visible l'information. Une analyse sociotechnique du traitement des données, *Réseaux*, 178-179, 2-3, 55-89.

110 Gelemerova L., 2009, On the Frontline against Money-Laundering: The Regulatory Minefield, *Crime, Law and Social Change*, 52, 33-55.

111 Gillespie T., 2014, The Relevance of Algorithms, *in* Gillespie T., Boczkowski P., Foot K. (Eds.), *Media Technologies: Essays on Communication, Materiality, and Society,* Cambridge, MA, MIT Press, 167-194.

112 Glouftsios Georgios., 2019, Designing Digital Borders The Visa Information System (VIS), *in* Hoijtink M., Leese M. (Eds.), *Technology and Agency in International Relations*, New York, Routledge, 164–188.

113 Glouftsios G., Leese M., 2023, Epistemic Fusion: Passenger Information Units and the making of international security, *Review of International Studies*, 49, 1, 125-142.

114 Grondin D., 2020, Biometric Algorithms as Border Infrastructures, *Public*, 30, 60, 62-75.

115 Grondin D., 2016, Mobilité, vie algorithmique et société de surveillance dans *Person of Interest*: la traque du national security state cyberspatial, *in* Lacroix I., Prémont K. (Eds.), *Représentations politiques, luttes de pouvoir et science-fiction,* Québec, Presses de l'Université du Québec, 165-202.

116 Grondin D., Hogue S., 2024, Person of Interest as Media Technology of Surveillance: A Cautionary Tale for the Future of the National Security State With Diegetic Big Data Surveillance, Algorithmic Security, and Artificial Intelligence, *Television & New Media*, 25, 4, 334-351.

117 Gros F., Castillo M., Garapon A., 2008, De la sécurité nationale à la sécurité humaine, *Raisons politiques*, 4, 32, 5-7.

118 Gros F., 2019, *The Security Principle: From Serenity to Regulation*, New York, Verso.

119 Han J., Huang Y., Liu S., 2020, Artificial Intelligence for Anti-Money Laundering: a Review and Extension, *Digital Finance*, 2, 211-239.

120 Harvey J., Lau S., 2009, Crime-money, Reputation and Reporting, *Crime, Law and Social Change*, 52, 57-72.

121 Hecht G., 2011, Introduction, *in* Hecht G. (Eds.), *Entangled Geographies: Empire and Technopolitics in the Global Cold War,* Cambridge, M, MIT Press, 1-12.

122 Hildebrandt M., 2018, Algorithmic regulation and the rule of law. *Philosophical of the Royal Society A*, 376, 2128, 1-11.

123 Huysmans J., 2014, *Security Unbound: Enacting Democratic Limits*, Abingdon, UK, Routledge.

124 Kaufmann M., 2024, AI in Policing and Law Enforcement, *in* Paul R., Carmel E., Cobbe J. (Eds.), *Handbook on Public Policy and Artificial Intelligence*, Elgaronline, 295-306.

125 Kaufmann M, Egbert S, Leese M., 2019, Predictive Policing and the Politics of Patterns, *The British Journal of Criminology*, 59, 3, 674-692.

126 Kitchin R., 2017, Thinking Critically about and Researching Algorithms, *Information, Communication and Society*, 20, 1, 14-29.

127 Kotef H., 2015, *Movement and Ordering of Freedom: On Liberal Governances of Mobility*, Durham, London, Duke University Press.

128 Johns F., Compton C., 2022, Data Jurisdictions and Rival Regimes of Algorithmic Regulations, *Regulation & Governance*, 16, 1, 63-84.

129 Larkin B., 2013, The Politics and Poetics of Infrastructure, *Annual Review of Anthropology*, 42, 1, 327-343

130 Leese M., 2024, Staying in Control of Technology: Predictive Policing, Democracy, and Digital Sovereignty, *Democratization*, 31, 5, 963-978.

131 Leese M., Wittendorp S. (Eds.), 2017, *Security/Mobility: Politics of Movement*, Manchester, Manchester University Press.

132 Leigh Star S., 1999, The Ethnography of Infrastructure, *American Behavioral Scientist*, 43, 3, 377-391.

133 Lokanan M.E., 2022, Predicting Money Laundering Using Machine Learning and Artificial Neural Networks Algorithms in Banks, *Journal of Applied Security Research*, 19, 1, 20-44.

134 Lyon D., 2022, Surveillance, Internet Policy Review, 11, 4, 1-18.

135 Lyon D., 2014, Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique, *Big Data and Society*, 1.

136 Lyon D. (Ed.), 2003, *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination*, New York, Routledge.

137 Lyon D., Murakami Wood D. (Eds.), 2021, *Big Data Surveillance and Security Intelligence: The Canadian Case*, Vancouver, University of British Columbia Press.

138 Masco J., 2014, *The Theater of Operations: National Security Affect from the Cold War to the War on Terror*, Durham, NC, Duke University Press.

139 McDaniel J., Pease K., 2021, *Predictive Policing and Artificial Intelligence*, New York, Routledge.

140 Narita K., An infrastructural approach to the digital Hostile Environment, *Journal of Global Ethics*, 19, 3, 294-306.

141 NICE Actimize, 2024a, *Transforming Transaction Monitoring and Reporting of Suspicious Activity*. https://fr.niceactimize.com/

142 NICE Actimize, 2024b, *Fighting Financial Crime*. https://fr.niceactimize.com/

143 Nøkleberg M., 2022, Expecting the Exceptional in the Everyday: Policing Global Transportation Hubs, *Security Dialogue*, 53, 2, 164-181.

144 Nolte A., Westermeier C., 2020, Between Public and Private: The Co-Production of Infrastructural Security, Politikon, 47, 1, 62–80.

145 Norris C., 2003, From Personal to Digital: CCTV, the Panopticon, and the Technological Mediation of Suspicion and Social Control, *in* Lyon D. (Eds.), *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination,* 249-281.

146 Pasquale F., 2015, *The Black Box Society: The Secret Algorithms That Control Money and Information*, Cambridge, MA, Harvard University Press.

147 Peters J.D., 2015, *The Marvelous Clouds: Toward a Philosophy of Elemental Media*, Chicago, University of Chicago Press.

148 Peeters M., Schuilenburg R. (Eds.), 2021, *The Algorithmic Society. Technology, Power, and Knowledge*, New York, Routledge.

149 Picaud M., Adam M., 2024, « Fini de jouer ». Entretien sur la sécurité dans les cercles anti-Jeux olympiques et paralympiques Paris 2024, *Métropoles*, 34.

150 Roberge J., Seyfert R., 2016, Introduction, *in* Roberge J., Seyfert R. (Eds.), *Algorithmic Cultures: Essays on Meaning, Performance and New Technologies,* New York, Routledge, 1-25.

151 Rossiter N., 2016, *Software, Infrastructure, Labor: A Media Theory of Logistical Nightmares*, New York, Routledge.

152 Rouvroy A., 2016, *Des données et des Hommes. Droits et libertés fondamentales dans un monde de données massives*, Strasbourg, Conseil de l'Europe.

153 Rouvroy A., Berns T., 2013, Gouvernementalité algorithmique et perspectives d'émancipation: le disparate comme condition d'individuation par la relation ?, *Réseaux*, 177, 1, 163-196.

154 Ruppert E., 2012, The Governmental Topologies of Database Devices, *Theory, Culture and Society*, 29, 4-5, 116-136.

155 Shapiro A., 2019, Predictive Policing for Reform ? Indeterminacy and Intervention in Big Data Policing, *Surveillance & Society*, 17, 3-4, 456-472.

156 Singh C., Lin W., 2021, Can Artificial Intelligence, RegTech and CharityTech Provide Effective Solutions for Anti-Money Laundering and Counter-Terror Financing Initiatives in Charitable Fundraising, *Journal of Money Laundering Control*, 24, 3, 464-482.

157 Ulbricht L., Yeung K., 2022, Algorithmic Regulation: A maturing Concept for Investigating Regulation of and tAlgorithms, *Regulation & Governance*, 16, 1, 3-22.

158 Westermeier C., 2023, From flows towards updates: Security regimes and changing technologies for financial surveillance, *Review of International Studies*, 49, 4, 615-636.

159 Weber J., Follis K., Suchman L., 2017, Tracking and Targeting: Sociotechnologies of (In)security, *Science, Technology, and Human Values*, 42, 6, 983-1002.

160 Waterton C., 2010, Experimenting with the Archive: STS-ers as Analysts and Co-constructors of Databases and Other Archival Forms, *Science, Technology, & Human Values*, 35, 5, 645-676.

161 Wessels M., 2023, Algorithmic Policing Accountability: Eight Sociotechnical Challenges, *Policing and Society*, 34, 3, 124-138.

162 Yeung K., 2017, Algorithmic Regulation: A Critical Interrogation, *Regulation & Governance*, 12, 4, 505-523.

163 Yeung K., Lodge M. (Eds.), 2019, *Algorithmic Regulation*, Oxford, Oxford University Press.

NOTES

1. Suivant Barocas *et al*. (2014), nous pouvons définir de façon provisoire et schématique la notion d'algorithme comme « une séquence formellement spécifiée d'opérations logiques qui fournit des instructions étape par étape à des ordinateurs pour agir sur des données et ainsi automatiser des décisions ». En complément, selon Dominique Cardon (2012), « comme la recette de cuisine, un algorithme est une série d'instructions permettant d'obtenir un résultat. À très grande vitesse, il opère un ensemble de calculs à partir de gigantesques masses de données (les '*big data*') ».

2. Cet article fait ainsi directement écho à deux autres textes publiés en anglais : Amicelle, A., 2022, Big data surveillance across fields: Algorithmic governance for policing & regulation, *Big Data & Society*, 9, 2 ; Amicelle A., Grondin D., 2021, Algorithms as suspecting machines: Financial surveillance for security intelligence, *in* Lyon D., Murakami Wood D. (Eds.), *Big Data Surveillance and Security Intelligence: The Canadian Case*, Vancouver, University of British Columbia Press, 68-87.

1. Forgé par Robert Clarke dès la fin des années 1980, ce néologisme caractérise « *le recours méthodique à des systèmes de données personnelles pour enquêter ou surveiller les actions ou les communications d'une ou plusieurs personnes* » (Clarke, 1988, 499). Il souligne autant qu'il anticipe l'importance prise par les bases de données et les logiciels informatiques en matière de surveillance.

2. Pour une analyse critique de ce programme et de ces équivalents, voir Amicelle, 2014; Westermeier, 2023.

1. Sur la question des « biais encodés » et des discriminations qui en découlent, voir également Benjamin, 2019.

1. « Biens appartenant à un groupe terroriste : Une déclaration de biens appartenant à un groupe terroriste doit être transmise à Canafe immédiatement, lorsqu'une entité déclarante est tenue de faire une communication à la GRC [Gendarmerie Royale du Canada] ou au SCRS [Service Canadien du Renseignement de Sécurité] en vertu du Code criminel ou du Règlement d'application des résolutions des Nations Unies sur la lutte contre le terrorisme. Contrairement aux autres types de déclarations transmises à Canafe, il n'est pas nécessaire qu'une opération soit effectuée ou tentée pour soumettre une déclaration de biens appartenant à un groupe terroriste ». https://fintrac-canafe.canada.ca/individuals-individus/rpt-fra

RÉSUMÉS

La montée en puissance de l'intelligence artificielle et des algorithmes comme nouvelles figures du pouvoir de surveiller et d'agir à partir de vastes masses de données est devenu un enjeu incontournable en matière de sécurité et de contrôle social. Au cours des vingt dernières années, soit la période d'existence de *Champ Pénal*, ce sujet a en effet pris une importance considérable. Pourtant, il brille paradoxalement par son absence dans les publications de la revue. Alors que le numéro anniversaire constitue une occasion idéale pour commencer à y remédier, le présent

article vise à poser un premier jalon en ce sens, et ce à la lumière des systèmes algorithmiques de surveillance et de suspicion déployés dans le cadre de la politique mondiale contre l'argent sale.

The rise of artificial intelligence and algorithms as key actants to monitor and act on the basis of big data for security and social control purposes has become critical over the last twenty years, i.e. since the creation of the journal Penal Field. Yet, paradoxically, this highly topical phenomenon is largely absent from the journal's publications. While the 20th anniversary special issue provides the ideal opportunity to begin to remedy this, the present article aims to take a first step in this direction, in the light of the algorithmic systems of surveillance and suspicion deployed in the name of the global policy against dirty money.

INDEX

Mots-clés : algorithmes, argent sale, mobilité, policing, régulation, sécurité, surveillance, suspicion
Keywords : algorithms, dirty money, mobility, policing, regulation, security, surveillance, suspicion

AUTEURS

ANTHONY AMICELLE

Maître de conférences, Centre Émile Durkheim, Sciences Po Bordeaux. Contact : a.amicelle@sciencespobordeaux.fr

DAVID GRONDIN

Professeur titulaire, département de communication de l'Université de Montréal. Contact : david.grondin.2@umontreal.ca