Suivre l'argent au XXIe siècle. Le devoir de vigilance numérique au nom de la sécurité publique

Anthony Amicelle

Cahiers Droit, Sciences & Technologies

20 | 2025
Vigilance dans le milieu numérique et normes juridiques

Suivre l'argent au XXIe siècle

Le devoir de vigilance numérique au nom de la sécurité publique

Anthony Amicelle

Édition électronique
URL : https://journals.openedition.org/cdst/12055
DOI : 10.4000/147zp
ISSN : 2431-8663

Éditeur
Presses universitaires d'Aix-Marseille - PUAM

Édition imprimée
Date de publication : 23 juin 2025
Pagination : 59-68
ISSN : 1967-0311

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

Référence électronique
Anthony Amicelle, « Suivre l'argent au XXIe siècle », *Cahiers Droit, Sciences & Technologies* [En ligne], 20 | 2025, mis en ligne le 28 juin 2025, consulté le 11 juillet 2025. URL : http://journals.openedition.org/cdst/12055 ; DOI : https://doi.org/10.4000/147zp

Suivre l'argent au XXIe siècle

Le devoir de vigilance numérique au nom de la sécurité publique

Anthony Amicelle*

Résumé : Au cours des dernières décennies, « suivre l'argent » (*Follow-the-money*) s'est imposé comme le mot d'ordre de la principale politique mondiale contre la criminalité, et le fondement d'un des plus importants programmes de surveillance antiterroristes. L'objectif du présent article est de rendre compte des conditions d'application de ce mot d'ordre – et leurs conséquences multiples – dans le cadre de dispositifs de vigilance numérique reposant avant tout sur l'enrôlement d'organisations qui ne sont ni des services de police et de renseignement, ni des sociétés de sécurité privée.

Mots-clés : vigilance numérique, argent, criminalité, sécurité, terrorisme

Abstract: *Over the last decades, « follow-the-money » has become the motto of the main global policy against crime, and one of the most important surveillance programs against terrorism. The aim of this article is to question the concrete implementation – and multiple consequences – of such a motto in the context of digital vigilance apparatuses primarily based on the enlistment of organizations that are neither police and intelligence services, nor private security companies.*

Keywords: *digital vigilance, money, crime, security, terrorism*

« Je dirais "suivez l'argent, Earl, car c'est là que cela va se passer". Malheureusement, nous n'avons pas été en mesure de suivre l'argent par le passé car les documents étaient soit inexistants, soit détruits. » Cette phrase est généralement considérée comme la première occurrence officielle d'une expression qui a depuis fait florès : « *follow the money* ». Elle a été prononcée aux États-Unis par le ministre adjoint de la Justice en juin 1974, lors des auditions en commission sénatoriale pour la nomination d'Earl J. Silbert comme premier procureur dans le cadre du « scandale du Watergate » ayant mené à la démission du président Richard Nixon[1]. Cette expression a ensuite été popularisée à l'occasion de la sortie du film oscarisé *Les Hommes du Président / All the President's Men*[2], tiré du best-seller éponyme des journalistes Carl Bernstein et Bob Woodward à l'origine du scandale.

• Maître de conférences en science politique à Sciences Po Bordeaux et professeur associé à l'université de Montréal.

1 R. Huret, *De l'Amérique ordinaire à l'État secret. Le cas Nixon*, Paris, Presses de Sciences Po, 2009.

2 A. Pakula, *All the President's Men*, États-Unis, Wilwood Enterprises, 1976.

Quarante ans plus tard, selon les normes internationales et les législations pénales en vigueur, « il faut suivre l'argent » afin de réprimer un large ensemble d'activités criminelles, de traquer des individus et des groupes désignés comme terroristes, et de prévenir la prolifération des armes de destruction massive. Dans cette perspective, des dispositifs de vigilance ont été mis en place et, malgré des différences d'échelle et d'approche, ils partagent deux points communs. Premièrement, ces dispositifs donnent concrètement lieu à des pratiques quotidiennes de surveillance financière de plus en plus médiées par des technologies numériques, qu'il s'agisse d'instruments algorithmiques de suspicion ou de systèmes de *dataveillance* fondés sur la collecte massive de données commerciales. Deuxièmement, l'opérationalisation de cette surveillance financière *high-tech* repose avant tout sur l'enrôlement d'organisations qui ne sont ni des services de police et de renseignement, ni des sociétés de sécurité privée. À partir d'un programme de recherche mené au cours des dix dernières années en Europe et en Amérique du Nord, et dont les résultats seront mobilisés au fur et à mesure par des références à des publications antérieures, le présent article a pour objectif de rendre compte des principaux enjeux et usages de ces dispositifs de vigilance numérique à l'interface de la finance et de la sécurité.

I. Suivre l'argent dans les sociétés numériques

> « Dans un monde globalisé où la technologie permet à l'argent de circuler partout rapidement, lutter contre le blanchiment d'argent est plus urgent que jamais. Des trillions de dollars sont blanchis chaque année. Cet argent alimente la grande criminalité. #*FollowTheMoney*[3] ».

Cet extrait de citation est issu d'une campagne publique de sensibilisation contre l'argent sale lancée par le GAFI – Groupe d'action financière –, l'organisation internationale de référence en la matière[4]. Initiée au sortir des années 1980, cette lutte contre l'argent sale a progressivement pris la forme d'une politique dite globale, officiellement appliquée dans plus de deux cents pays et territoires, et couvrant tout type de crime associé à des flux financiers illicites, du vol simple aux grands trafics en passant par les illégalismes des élites dirigeantes, ainsi que le financement du terrorisme et de la proliferation nucléaire. En pratique, cette politique se traduit au quotidien par l'exercice d'une surveillance financière, dans le but affiché de détecter et de signaler des transactions suspectes au nom du maintien de l'ordre public et de la sécurité (inter) nationale[5]. Mais qu'est-ce qu'une « transaction suspecte » ? Qui « suit l'argent » ? Et comment dans un monde dit globalisé et *high-tech* ?

---

3 Lien vers la campagne vidéo du Gafi : <https://www.youtube.com/watch?v =T1_1hnLbCI0>.

4 M.T. Nance, « The regime that FATF built : An introduction to the financial action task force », *Crime, Law and Social Change* 2018, 69(2), p. 109-129.

5 J. Harvey & S. F. Lau, « Crime-money, reputation and reporting », *Crime, Law and Social Change* 2009, 52, p. 57-72 ; C. King, C. Walker & J. Gurule (eds.), *The Palgrave Handbook of Criminal and Terrorism Financing Law*, Cham, Palgrave Macmillan, 2018.

Ce devoir de vigilance financière est la responsabilité de toute une série d'acteurs et de secteurs économiques, à commencer par les banques et l'industrie financière en tant que « partenaires réticents » enrôlés pour mettre sous surveillance ce qu'ils ont pour vocation de mettre en circulation, l'argent[6]. Pour rendre compte de cette obligation légale, d'aucuns l'inscrivent dans

> « une chaîne de sécurité, au sein de laquelle des données commerciales sont analysées, collectées, signalées, partagées, transférées, et finalement utilisées comme base d'intervention policière et judiciaire. Dans ce contexte, des compagnies privées – dont Facebook et Twitter, des compagnies aériennes et des banques – se retrouvent en première ligne contre le terrorisme et d'autres menaces à la sécurité[7] ».

Nombre de configurations d'action publique de sécurité dépendent ainsi d'acteurs majeurs du capitalisme contemporain qui ne sont pas des sociétés de sécurité privée à proprement parler, tels que des institutions financières, des plateformes de réseaux sociaux[8], ou encore des compagnies de transport et de logistique[9]. Contrairement aux prestataires de services de sécurité dont ces entreprises sont elles-mêmes clients, le contrôle du crime n'est ni le cœur de métier ni une source directe de profit et d'accumulation du capital. Elles ne correspondent tout simplement pas au canon de la police privée, qui renvoie aux « diverses formes légales et organisées de services marchands dont les principaux objectifs incluent la lutte contre la criminalité, la protection des biens et des personnes, et le maintien de l'ordre[10] ». En effet, ces entreprises sont avant tout positionnées dans des univers économiques et financiers relativement distincts de ceux de la sécurité et du pénal, et, par extension, des luttes de définition, de hiérarchisation et de gestion des crimes et désordres[11].

Dans cette perspective, tant la surveillance d'État au nom de la sécurité que la surveillance d'entreprise au nom de la rentabilité – en particulier à l'âge du capitalisme de surveillance[12] – sont des phénomènes bien identifiés dans le débat public.

---

6 G. Favarel-Garrigues, T. Godefroy & P. Lascoumes, « Reluctant partners? Banks in the fight against money laundering and terrorism financing in France », *Security Dialogue* 2011, 42(2), p. 179-196; E. Bosma, *Banks as security actors : Countering terrorist financing at the human-technology interface*, New York, Routledge, 2025.

7 M. de Goede, « The chain of security », *Review of International Studies* 2018, 44(1), p. 25.

8 V. Crosset & B. Dupont, « Cognitive assemblages : The entangled nature of algorithmic content moderation », *Big Data & Society* 2022, 9(2).

9 M. Nøkleberg, « Expecting the exceptional in the everyday, Policing global transportation hubs », *Security Dialogue* 2022, 53(2), p. 164-181. G. Glouftsios & M. Leese, « Epistemic fusion : Passenger Information Units and the making of international security », *Review of International Studies* 2023, 49(1), p. 125-142.

10 E. E. Joh, « The paradox of private policing », *The Journal of Criminal Law and Criminology* 2004, 95(1), p. 55.

11 D. Bigo, « Globalized (in)security : The field and the ban-opticon », *in* D. Bigo & A. Tsoukala (eds.), *Terror, Insecurity and Liberty,* Londres, Routledge, 2008, p. 10-48.

12 S. Zuboff, *The Age of Surveillance Capitalism*, New York, Public Affairs, 2019.

> « Mais le fait que des autorités gouvernementales et des établissements privés puisse participer ensemble à des "assemblages de surveillance" au nom d'objectifs partagés échappe [ou tout du moins a longtemps échappé] à un cadre d'analyse dans lequel les finalites dites étatiques et commerciales de la collecte de données personnelles semblent incompatibles[13]. »

Ainsi, les banques tendent encore à être exclusivement appréhendées comme des organisations auprès desquelles tout un chacun peut placer ou emprunter de l'argent, et non comme les yeux et les oreilles de l'État sécuritaire dans l'espace financier, en écho indirect aux appels à la vigilance citoyenne incitant à signaler toute activité suspecte, avec des campagnes du type « si vous vous voyez quelque chose, dîtes quelque chose[14] ». Or, là où ces appels et ces campagnes publiques tendent à promouvoir un « droit à la suspicion », il s'agit davantage d'un devoir pour les entreprises soumises aux obligations anti-blanchiment. Tout en restant des prestataires de services financiers pour le compte de leurs clients, les banques sont également devenues des organes de surveillance et de dénonciation pour le compte des forces de l'ordre et des agences de renseignement, avec à la clef plusieurs dizaines de millions de signalements par an dans certains pays occidentaux, incluant des centaines de milliers de « déclarations de soupçon[15] ».

Pour ce faire, la surveillance financière est opérée de trois manières différentes et complémentaires, de la surveillance au guichet – en face-à-face – jusqu'aux formes les plus récentes de *big dataveillance* à distance, avec l'accent mis sur le déploiement à la fois généralisé et ambivalent de « systèmes algorithmiques[16] ».

Premièrement, dans le cadre du devoir de vigilance contre l'argent sale[17], une partie de cette surveillance financière a toujours lieu « au guichet », au sein des agences bancaires où les clients sont susceptibles de se rendre pour effectuer des opérations financières. Aux fins de conformité anti-blanchiment et contre le financement du terrorisme, les employés de banque dits de première ligne, en contact direct avec la clientèle (du guichetier au gestionnaire de patrimoine), doivent suivre des formations internes dédiées à la détection d'opérations inhabituelles et suspectes[18]. Dans ce contexte, la surveillance

---

13 A. Amicele & G. Favarel-Garrigues, « Financial surveillance : Who cares ? », *Journal of Cultural Economy* 2012, 5(1), p. 117.

14 J. Reeves, *Citizen Spies. The Long Rise of America's Surveillance Society*, New York, New York University Press, 2017.

15 A. Amicelle, « Big data surveillance across fields. Algorithmic governance for policing and regulation », *Big Data & Society* 2022, 9(2).

16 L'expression « systèmes algorithmiques » fait référence aux 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 (R. Bellanova, K. Irion, K. L. Jacobsen *et al.*, « Toward a critique of algorithmic violence », *International Political Sociology* 2021, 15, p. 129.)

17 GAFI, Les recommandations du GAFI. Normes internationales sur la lutte contre le blanchiment de capitaux et le financement du terrorisme et de la proliferation, 2025.

18 G. Favarel-Garrigues, T. Godefroy & P. Lascoumes, « Sentinels in the banking industry, Private actors and the fight against money laundering in France », *The British Journal of Criminology* 2008, 48,

et, par extension, la suspicion portent principalement sur le comportement des clients en interaction avec ces banquiers de première ligne, et ce à l'aune de « signaux d'alerte potentielle » fournis par les autorités étatiques, comme au Canada[19], du type « le client a un comportement nerveux ». Il peut ainsi en découler des signalements internes aux banques qui font l'objet d'un traitement par des équipes d'analystes intégrés aux départements de conformité, afin de déterminer si ces signalements doivent donner lieu à des déclarations de soupçon auprès de l'autorité étatique compétente, à savoir la cellule nationale de renseignement financier, à l'instar de Tracfin en France, Fintrac au Canada, Austrac en Australie ou FinCEN aux États-Unis[20].

Deuxièmement, la surveillance financière est aussi associée à des pratiques de *risk scoring*. Cela se traduit par « une surveillance stratifiée : surveillant les individus de façon différenciée selon leur score de risque [ici d'argent sale][21] ». Contrairement à la surveillance en face-à-face au guichet, ce second modèle de surveillance indexé au risque est déployé à distance, sans aucune interaction ni observation directe de la clientèle dont les opérations financières sont ainsi placées sous vigilance renforcée. Cette surveillance à distance indexée au risque est effectuée « manuellement », sous la forme d'examens réguliers de l'historique numérisé des transactions et autres mouvements de capitaux des clients classés à haut-risque d'argent sale. L'objectif est toujours le même, à savoir détecter des activités inhabituelles et donc potentiellement suspectes, mais cette fois-ci à l'aune du comportement non plus interactionnel mais transactionnel de la clientèle contrôlée, avec des signaux d'alerte potentielle tels que : « l'activité transactionnelle (niveau et volume) ne correspond pas à la situation financière du client, à ses activités habituelles ou aux informations le concernant (par exemple étudiant, sans emploi, allocataire, etc.[22] ».

Au cours des dernières années, ces deux formes de surveillance financière ont progressivement été considérées insuffisantes au regard des nouvelles exigences internationales de « vigilance constante » à l'égard des relations d'affaires et des opérations effectuées dans ce cadre[23]. D'un côté, la surveillance au guichet est apparue par définition discontinue et partielle. Elle n'aurait lieu qu'à l'occasion d'interactions

---

p. 1-19 ; V. Iafolla, « The production of suspicion in retail banking : An examination of unusual transaction reporting », in C. King, C. Walker, & J. Gurule (eds.), *The Palgrave Handbook of Criminal and Terrorism Financing Law*, Cham, Palgrave Macmillan, 2018, p. 81-107.

19 FINTRAC, Guidelines. Guideline 2 : Suspicious Transactions, 2023.

20 V. Mitsilegas, « New forms of transnational policing : the emergence of financial intelligence units in the European Union and the challenges for human rights : Part 1 », *Journal of Money Laundering Control* 1999, 3(2), p. 147-160; P. Lagerwaard, « Financial surveillance and the role of the Financial Intelligence Unit (FIU) in the Netherlands », *Journal of Money Laundering Control* 2023, 26(7), p. 63-84; A. Amicelle, « Right of entry. The struggle over recognition in the world of intelligence », *Political Anthropological Research on International Social Sciences* 2020, 1(2), p. 243-272.

21 S. Brayne, « Big data surveillance : The case of policing », *American Sociological Review* 2017, 82(5), p. 989.

22 A. Amicelle, & V. Iafolla, « Suspicion-in-the-making : Surveillance and denunciation in financial policing », *The British Journal of Criminology* 2018, 58(4), p. 845-863.

23 GAFI, Les recommandations du GAFI. Normes internationales sur la lutte contre le blanchiment de capitaux et le financement du terrorisme et de la proliferation, 2025.

occasionnelles, et de plus en plus rare au regard de la baisse du nombre de visites et de rendez-vous en agences bancaires. De l'autre, la surveillance à distance indexée au risque est également apparue limitée dans la mesure où elle ne cible en moyenne qu'1 % de la clientèle, à savoir les clients classés à risque élevé en matière d'argent sale.

Dans ce contexte, une série d'instruments algorithmiques, plus ou moins sophistiqués[24], sont progressivement devenus les principaux actants de la surveillance financière au nom de la sécurité et de la lutte contre les crimes et désordres, et ce avec une évolution notable à trois niveaux.

Premièrement, ces instruments ont été déployés pour surveiller les transactions de tout le monde et à tout moment, que le client se présente au guichet ou non, et que son score de risque d'argent sale soit élevé ou non. Deuxièmement, leurs usages contribuent à renforcer la prédominance d'une forme de *dataveillance* transactionnelle. En effet, les critères relatifs aux comportements transactionnels y sont primordiaux – encore plus que dans le modèle de surveillance à distance indexé au risque – et peuvent même s'avérer suffisants dans nombre de cas pour générer des alertes quotidiennes, sans référence nécessaire au profil sociodémographique et financier du client visé. Troisièmement enfin, l'opération de surveillance tout comme les alertes qui en résultent sont dès lors automatisées, et non plus « manuelles » comme dans le cas des modèles de surveillance précédents (et toujours existants). Néanmoins, l'intervention humaine et les processus de décision attenants n'ont pas pour autant disparu, à l'instar de la plupart des configurations actuelles de *policing* et de sécurité algorithmique, aussi bien à l'échelle des patrouilles de police et des tribunaux civils et pénaux[25], qu'à celle des dispositifs de renseignement policier et des appareils de sécurité transnationaux[26]. Les instruments algorithmiques y sont ainsi généralement cantonnés au rôle de « systèmes de recommandation » pour les agents dont la responsabilité est d'analyser chaque alerte automatisée tout en effectuant des vérifications additionnelles en vue d'une décision finale[27].

À la lumière de l'abondante littérature interdisciplinaire sur les systèmes algorithmiques de policing, de renseignement et de sécurité au sens large, le constat de leur usage répandu et toujours croissant en matière de surveillance financière n'apparaît pas comme une surprise empirique. En revanche, leur relative simplicité de fonctionnement en est une, en profond décalage autant avec les discours publics que les études théoriques si ce n'est

---

24 A. Amicelle, & D. Grondin, « Algorithms as suspecting machines : Financial surveillance for security intelligence », in D. Lyon & D. Murakami Wood (eds.), *Big Data Surveillance and Security Intelligence* : *The Canadian Case,* Vancouver, University of British Columbia Press, 2021, p. 68-87.

25 B. Benbouzid, « To predict and to manage. Predictive policing in the United States », *Big Data & Society* 2019, 6(1); S. Brayne & A. Christin, « Technologies of crime prediction », *Social Problems* 2021, 68(3), p. 608-624.

26 J. Chan & L. Bennett Moses, « Making sense of big data for security », *The British Journal of Criminology* 2017, 57(2), p. 299-319; D. Bigo & L. Bonelli, « Digital data and the transnational intelligence space », in D. Bigo, E. Isin, & E. Ruppert (eds.), *Data Politics* : *Worlds, Subjects, Rights,* Londres, Routledge, 2019, p. 100-122.

27 R. Bellanova & M. de Goede, « The algorithmic regulation of security : An infrastructural perspective », *Regulation & Governance* 2022, 16(1), p. 102-118.

spéculatives sur l'intelligence artificielle dans le domaine des technologies de sécurité. Jusqu'à présent, les programmes dits de *big dataveillance* financière sont principalement basés sur des modèles de règles prédéfinies du type « Si… alors[28] », loin de ce que Daniel Neyland a récemment pu dépeindre avec une certaine ironie critique comme une sorte de « drama algorithmique dans la recherche universitaire actuelle[29] ». Cette situation de simplicité et de limitation relatives des instruments algorithmiques illustre la tension structurelle propre aux configurations de sécurité contemporaines fondées sur la mise en relation d'univers de pratiques et de rationalités différenciées, de la banque et la finance à la sécurité nationale et au pénal en passant par la régulation économique. *In fine*, si cela conduit bien au quotidien à une surveillance financière automatisée de masse, celle-ci apparaît pourtant très éloignée tant des ambitions affichées en matière de contrôle du crime que des visions dystopiques liées au *big data*, avec par ailleurs des conséquences plus que limitées sur l'ordre financier existant.

Outre cette politique globale contre l'argent sale, la mise en priorité de la question du financement du terrorisme dans le contexte de la « Guerre contre la terreur » a également donné lieu à une autre forme de vigilance numérique *via* des pratiques massives de surveillance financière.

II. *Dataveillance* financière transnationale au nom de l'antiterrorisme

« En suivant l'argent, le TFTP a permis aux États-Unis et à leurs alliés d'identifier et de localiser des agents et leurs soutiens financiers, de cartographier des réseaux terroristes, et d'empêcher que l'argent ne tombe entre leurs mains[30]. » Il s'agit d'un extrait de la présentation officielle du programme américain de traque du financement du terrorisme (*TFTP-Terrorist Finance Tracking Program*) sur le site du Trésor, près de 25 ans après sa mise en place en octobre 2001 et 18 ans après la révélation controversée de son existence dans les médias[31]. En tant que programme inédit en matière de *dataveillance* financière au nom de la sécurité nationale, la condition de possibilité du TFTP peut être résumée en un mot : traçabilité. Selon Marie-Angèle Hermitte :

> « La surveillance, vieille réalité, ne devient la moderne traçabilité que lorsqu'elle s'exerce au sein d'un système organisé, dont l'extension laisse à

28 A. Amicelle, « Big data surveillance across fields. Algorithmic governance for policing and regulation », art. cité.

29 D. Neyland, *The Everyday Life of an Algorithm*, New York, Palgrave Macmillan, 2019, p. 81.

30 V. le site du Trésor américain dédié au programme de traque du financement du terrorisme : <https://home.treasury.gov/policy-issues/terrorism-and-illicit-finance/terrorist-finance-tracking-program-tftp>.

31 G. Gonzalez Fuster, P. De Hert & S. Gutwirth, « SWIFT and the vulnerability of transatlantic data transfers », *International Review of Law Computers & Technology* 2008, 22(1-2), p. 191-202; A. Amicelle, « The great (data) bank robbery : The terrorist finance tracking program & the "SWIFT Affair" », *Research Questions* 2011, 36, p. 1-27 ; M. Wesseling, M. De Goede & L. Amoore, « Data wars beyond surveillance, Opening the black box of SWIFT », *Journal of Cultural Economy* 2012, 5(1), p. 49-66.

> penser qu'il s'agit d'un véritable projet de société, poursuivi autant par des pouvoirs privés que par les pouvoirs publics[32] ».

Concernant les flux financiers transnationaux, un tel système organisé de traçabilité a d'abord été mis en place par la *Society for Worldwide Interbank Financial Telecommunication*, communément appelée par son acronyme SWIFT, soit la principale plateforme de communication financière au monde, par laquelle transitent plus de 80 %[33] des transactions internationales. Ce système organisé a ensuite été dupliqué par l'administration américaine dans le cadre de la guerre contre le terrorisme.

> « Parler de traçabilité implique que soient réunis trois éléments : il faut qu'il y ait des traces et donc un support qui permette de les repérer ; il faut qu'il y ait un mécanisme de recueil de traces ; il faut enfin une structure qui permette de les traiter, de les analyser pour en tirer des conclusions. Sans ce type d'organisation, qui implique un volontarisme plus ou moins affirmé, les traces existent en fait, pas la traçabilité[34]. »

La plateforme de messagerie SWIFT est utilisée par 11 000 institutions financières dans plus de 200 pays et territoires, avec l'envoi quotidien de plus de 40 millions de communications, pour un total supérieur à 8 milliards de messages financiers au cours de l'année 2023. Dans ce contexte, un système de traçabilité financière a été organisé par SWIFT à des fins commerciales. En effet, chaque envoi de message produit des traces numériques qui sont temporairement collectées et stockées dans les bases de données de la société, avec une infrastructure sociotechnique permettant de rechercher et d'analyser les traces ciblées. En cas de problème imprévu ou de demande spécifique des institutions financières clientes, SWIFT est dès lors en mesure de retrouver la trace numérique des transactions internationales ayant transité par sa plateforme. Les trois éléments nécessaires à la traçabilité sont ainsi combinés pour assurer la qualité du service mondial de messagerie systémique offert.

En octobre 2001, ce système organisé de traçabilité à finalité commerciale s'est superposé avec la volonté émise au sein de l'administration américaine de se doter d'un tel système, cette fois-ci avec une finalité orientée vers la sécurité nationale. C'est l'acte de naissance du programme de traque du financement du terrorisme fondé sur un détournement d'usage des traces numériques générées par la messagerie interbancaire de SWIFT[35]. Cet enjeu de détournement d'usage ou d'usage secondaire renvoie donc à

---

32 M.-A. Hermitte, « La traçabilité des personnes et des choses. Précaution, pouvoirs et maîtrise », in P. Pedrot (ed.), *Traçabilité et responsabilité,* Paris, Economica, 2003, p. 3.

33 A. Amicelle, « (Il)légitimité du renseignement financier : usages transnationaux de la traçabilité des flux de capitaux », *Criminologie* 2014, 47(2), p. 77-104.

34 *Ibid.*

35 A. Amicelle, « The EU's paradoxical efforts at tracking the financing of terrorism. From criticism to imitation of dataveillance », *Liberty and Security Series* 2013, 56, p. 1-19 ; M. de Goede & M. Wesseling, « Secrecy and security in transatlantic terrorism finance tracking », *Journal of European Integration* 2017, 39(3), p. 253-269.

des informations collectées pour une finalité donnée, mais qui se voient réutilisées pour une autre finalité sans le consentement explicite des personnes concernées[36]. Les agents du Trésor américain ont justifié cet accès et ce traitement de données massives, en lien avec un nombre considérable de messages numériques SWIFT, au nom d'une logique préemptive, afin de désorganiser et de mettre en incapacité des suspects de terrorisme avant même qu'ils n'aient pu agir par le biais d'attaques violentes. Plus précisément, deux principaux narratifs de légitimation ont été mobilisés pour promouvoir la valeur ajoutée de la surveillance financière opérée via le TFTP.

D'une part, à l'instar d'autres programmes de sécurité reposant sur des capacités de *dataveillance*, l'accent mis sur le TFTP a été associé à la possibilité de mettre en relation une série de mobilités (financières et humaines), avec en particulier l'idée de suivre l'argent à la trace numérique pour retrouver et suivre la trace cette fois-ci physique de suspects en mouvement. Selon le discours officiel régulièrement répété et abondamment repris à cet égard,

> « par exemple, il est possible de localiser un suspect en vérifiant quand et où le suspect a fermé et/ou ouvert un nouveau compte bancaire dans une ville ou un pays autre que son dernier lieu de résidence connu. Ceci est un indicateur clair que l'individu a pu bouger. [...] Le programme de traque du financement du terrorisme peut fournir des informations capitales sur les mouvements de suspects terroristes et sur la nature de leurs dépenses[37] ».

En d'autres termes, sur la base des traces numériques, la valeur ajoutée serait de tracer les flux financiers pour traquer les suspects de terrorisme. D'autre part, le programme a été promu pour cartographier des réseaux terroristes. Comme l'a rappelé Marieke de Goede dans sa critique des pratiques de surveillance financière, la connectivité par l'argent est ici pensée comme le liant, c'est-à-dire l'élément qui fait tenir un réseau terroriste dans son ensemble et, à ce titre, elle est considérée comme une source majeure de renseignement[38]. Cette primauté accordée aux relations financières produit en retour du soupçon par association[39]. Avoir envoyé ou reçu de l'argent de la part d'un suspect de terrorisme connu engendre des doutes si ce n'est des soupçons caractérisés sur la personne concernée.

Bien que l'efficacité et la régulation – au travers d'accords États-Unis/Union européenne – de ce programme de surveillance financière de masse soient toujours une source de débat, notamment en termes de respect de la vie privée et des droits

---

36 D. Solove. « I've got nothing to hide' and other misunderstandings of privacy », *San Diego Law Review*, 2007, 44, p. 745-772.

37 European Commission, *Joint Report from the Commission and the U.S. Treasury Department regarding the Value of TFTP Provided Data*, Bruxelles, 2013, p. 5.

38 M. de Goede, « Fighting the network : A critique of the network as a security technology », *Distinktion* 2012, 13(3), p. 215-232.

39 A. Amicelle, « (Il)légitimité du renseignement financier. Usages transnationaux de la traçabilité des flux de capitaux », *Criminologie* 2014, 47(2), p. 77-104.

fondamentaux, d'asymétrie informationnelle entre États souverains, de manque d'effectivité préemptive et de valeur-ajoutée finalement discutable, le TFTP perdure depuis 2001, soit quasiment depuis le début du XXIe siècle.

* * *

Au cours des dernières décennies, « suivre l'argent » est donc devenu le slogan officiel de la principale politique globale contre la criminalité, et le fondement d'un des plus importants programmes antiterroristes à ce jour. À ce double titre, si le *policing* (en tant qu'action de faire la police au sens large) renvoie « à la création de systèmes de surveillance couplée à la menace de sanctions en cas de deviance – soit immédiatement soit en lançant des procédures pénales[40] », alors une des spécificités du *policing* contemporain consiste en l'importance croissante accordée aux systèmes de surveillance financière au nom d'un devoir de vigilance appliqué aux banques et à un ensemble d'acteurs économiques de premier plan. Il en ressort que les configurations nationales et transnationales de *policing* dépendent de plus en plus d'une surveillance financière digitalisée. Cette dernière est opérée par et au sein d'organisations majeures du capitalisme contemporain, dont la rationalité économique est, de prime abord, relativement éloignée des logiques pénales et sécuritaires. Enfin, il apparaît que l'interventionnisme étatique dans la collecte, le stockage et le traitement de grandes messages de données numériques inhérentes au fonctionnement de la finance globale est une stratégie formellement privilégiée pour prendre et orienter une série de décisions en matière de sécurité nationale. Dans ce cadre, se demander qui peut bien se soucier de la surveillance financière – *financial surveillance : who cares ?*[41] ne devrait désormais plus être une question de recherche pertinente.

40 R. Reiner, *The Politics of the Police*, Oxford, Oxford University Press, 4th ed., 2010, p. 5.

41 A. Amicele & G. Favarel-Garrigues, « Financial surveillance : Who cares ? », *Journal of Cultural Economy* 2012, 5(1), p. 105-124.