Criminologie

(Il)légitimité du renseignement financier
Usages transnationaux de la traçabilité des flux de capitaux

Anthony Amicelle

Volume 47, numéro 2, automne 2014

Criminalité et police transnationales : une perspective critique

URI : https://id.erudit.org/iderudit/1026729ar
DOI : https://doi.org/10.7202/1026729ar

Aller au sommaire du numéro

Éditeur(s)

Les Presses de l'Université de Montréal

ISSN

0316-0041 (imprimé)
1492-1367 (numérique)

Découvrir la revue

Citer cet article

Amicelle, A. (2014). (Il)légitimité du renseignement financier : usages transnationaux de la traçabilité des flux de capitaux. *Criminologie*, *47*(2), 77–104. https://doi.org/10.7202/1026729ar

Résumé de l'article

Cet article est consacré à un enjeu encore trop peu étudié malgré son importance croissante dans un domaine tel que le policing transnational, à savoir le renseignement financier. Afin de contribuer à la réflexion sur cette composante à part entière des pratiques contemporaines de surveillance ou plutôt de dataveillance, l'analyse porte plus précisément sur le programme américain de traque du financement du terrorisme (*Terrorist Finance Tracking Program [TFTP]*). Fondé sur un espace de relations à la fois au-dessus, au-delà et en deçà du national, ce programme de sécurité participe à la production de renseignement à partir d'un dispositif de traçabilité des flux financiers. Il s'agit ici d'expliciter les conditions d'existence d'un tel dispositif consistant à mobiliser de larges ensembles de traces numériques générés par une forme particulière de circulation transfrontière. Il s'agit aussi de mettre la légitimité du TFTP à l'épreuve des narratifs de justification et des « réussites » qui lui sont associés.

(Il)légitimité du renseignement financier

Usages transnationaux de la traçabilité des flux de capitaux

Anthony Amicelle[1]
Professeur adjoint
École de criminologie, Université de Montréal
anthony.amicelle@umontreal.ca

RÉSUMÉ • *Cet article est consacré à un enjeu encore trop peu étudié malgré son importance croissante dans un domaine tel que le* policing *transnational, à savoir le renseignement financier. Afin de contribuer à la réflexion sur cette composante à part entière des pratiques contemporaines de surveillance ou plutôt de* dataveillance*, l'analyse porte plus précisément sur le programme américain de traque du financement du terrorisme (*Terrorist Finance Tracking Program [TFTP]*). Fondé sur un espace de relations à la fois au-dessus, au-delà et en deçà du national, ce programme de sécurité participe à la production de renseignement à partir d'un dispositif de traçabilité des flux financiers. Il s'agit ici d'expliciter les conditions d'existence d'un tel dispositif consistant à mobiliser de larges ensembles de traces numériques générés par une forme particulière de circulation transfrontière. Il s'agit aussi de mettre la légitimité du TFTP à l'épreuve des narratifs de justification et des « réussites » qui lui sont associés.*

MOTS-CLÉS • *Renseignement financier, traçabilité, surveillance, sécurité nationale, antiterrorisme.*

Introduction

HUMINT (*Human Intelligence*) ; TECHINT (*Technical Intelligence*) ; IMINT (*Imagery Intelligence*) ; COMINT (*Communications Intelligence*) ; TELINT (*Telemetry Intelligence*) ; ELINT (*Electronic Intelligence*) ; RADINT (*Radar*

1. Université de Montréal, École de criminologie, Pavillon Lionel-Groulx, C. P. 6128, succursale Centre-ville, Montréal, (Québec), Canada, H3C 3J7.

Intelligence) ; SIGINT (*Signals Intelligence*) ; MASINT (*Measurement & Signature Intelligence*) ; FISINT (*Foreign Instrumentation Signals Intelligence*) ; OSINT (*Open Source Intelligence*) ; GEOINT (*Geospatial Intelligence*) ; SOCMINT (*Social Media Intelligence*) ; FININT (*Financial Intelligence*).

Parmi la myriade d'acronymes mobilisée pour différencier les sources et méthodes de renseignement, les représentants du Trésor américain se sont saisis du sigle FININT en affirmant le rôle de leur département en matière antiterroriste. Cet accent mis sur le renseignement financier est particulièrement prégnant dans les écrits d'anciens membres du Trésor ayant participé aux actions menées au lendemain des attentats du 11 septembre 2001. Dans une perspective hagiographique, plusieurs personnalités ont en effet publié des ouvrages et articles aux titres évocateurs à ce sujet, que ce soit David D. Aufhauser (ancien directeur juridique du Trésor) avec *Terrorist Financing : Foxes Run to Ground* (2003), John B. Taylor (ancien sous-secrétaire d'État aux affaires internationales au sein du Trésor) avec *Global Financial Warriors : The Untold Story of International Finance in the Post 9/11 World* (2007), John Cassara (ancien agent spécial détaché au bureau « financement du terrorisme et renseignement financier » du Trésor) avec *On the Trail of Terrorist Finance : What Law Enforcement and Intelligence Officers Need to Know* (2010) ou encore Juan C. Zarate (ancien secrétaire adjoint du Trésor sur les questions de financement du terrorisme et de crimes financiers) avec *Treasury's Warfare : The Unleashing of a New Era of Financial Warfare* (2013). Ce dernier a exposé avec force détails la vision du FININT qui anime, selon lui, le département du Trésor. Il s'est livré à un véritable plaidoyer en faveur d'une « *nouvelle discipline de collecte et d'analyse de renseignement financier* » (p.46).

> Dans son acception générale, le renseignement financier renvoie à n'importe quel fragment d'information – récupéré – qui révèle des transactions commerciales ou financières et des flux d'argent, des données relatives à des actifs et à des capitaux, ainsi que les relations financières et commerciales, et les intérêts d'individus, de réseaux et d'organisations. De telles informations peuvent se présenter sous différentes formes – des reçus froissés découverts dans les refuges des terroristes, les livres de comptes détaillés des hawaladars, les déclarations de soupçon venant des banques, et les enregistrements des virements électroniques transnationaux. […] La bonne information à propos d'un expéditeur ou d'un bénéficiaire de fonds peut ouvrir une fenêtre sur des réseaux plus larges ou identifier des liens invisibles. Si c'est au moment opportun et suffisamment spécifique, un tel

> renseignement peut aider à stopper des actes de terrorisme. (Zarate, 2013, pp. 46-48)

Une part significative des stratégies déployées en ce sens au cours des années 2000 a essentiellement renforcé et sensiblement reconfiguré des mécanismes préexistants tels que les dispositifs anti-blanchiment (Favarel-Garrigues, 2003 ; Levi, 2010 ; Sheptycki, 2000 ; Vlcek, 2008). À cet exercice somme toute classique de conversion-adaptation du déjà-là s'est ajoutée une série d'initiatives inédites, à commencer par la mise sur pied du programme de traque du financement du terrorisme sous l'égide du Trésor américain dès octobre 2001 (*Terrorist Finance Tracking Program* ; ci-après TFTP). Depuis le dévoilement de son existence par voie de presse en juin 2006 (Lichtblau & Risen, 2006), ce programme n'a cessé d'être porté en étendard par les représentants du Trésor afin de promouvoir sa légitimité contestée mais aussi pour asseoir celle de leur département dans le domaine de la sécurité nationale.

> Après les attentats terroristes du 11 septembre 2001, le département américain du Trésor a établi le programme de traque du financement du terrorisme pour identifier, traquer et poursuivre des terroristes – tels qu'Al-Qaida – et leurs réseaux. Le département américain du Trésor est particulièrement bien placé pour pister les flux de capitaux terroristes et contribuer plus largement aux efforts du gouvernement des États-Unis pour découvrir les cellules terroristes et cartographier les réseaux terroristes ici et partout dans le monde. (U.S. Treasury, 2013a, p. 1)

Le présent article est tourné vers l'étude de ce programme. Véritable tête de gondole du renseignement financier, le TFTP entre également en résonance avec les débats suscités par les révélations d'Edward Snowden sur la collecte et le traitement de larges ensembles de traces numériques à des fins de sécurité nationale (Bigo *et al.*, 2013). À ce titre, cet article vise à fournir des éléments de réponse à trois questionnements simples ayant d'importantes implications théoriques. Premièrement, quelles sont les conditions d'existence d'un tel programme de sécurité consistant à mobiliser les traces inhérentes à une forme particulière (ici financière) de circulation transfrontière ? Deuxièmement, comment la création et la subsistance d'un tel programme sont-elles justifiées par ses promoteurs ? Autrement dit, à quoi sert-il officiellement ? Quelle serait sa valeur ajoutée ? Troisièmement, « ne pas leur faire confiance serait leur faire offense » (Guittet, 2006), il s'agit de prendre au sérieux et d'analyser les exemples concrets donnés

par les défenseurs du programme pour appuyer leurs narratifs de légitimation. Nous nous attacherons tout d'abord à rendre compte du triple processus de numérisation, d'hybridation et de transnationalisation (Bauman *et al.*, 2014) sous-tendant la traçabilité des transactions financières internationales au nom de la lutte contre le terrorisme. Dans une seconde partie, nous insisterons sur la façon dont la logique préemptive est systématiquement articulée autour du triptyque « identifier, localiser et mettre en réseau », pour ensuite confronter cette rhétorique aux cas empiriques.

Avec ce texte, nous souhaitons ouvrir de nouvelles pistes de recherche tout en prolongeant celles explorées ces dernières années (Amicelle 2011, 2013a, 2013b), avec pour ambition de contribuer à une réflexion interdisciplinaire sur les enjeux de renseignement financier. Afin de compenser au mieux l'impossibilité d'accéder aux principaux « acteurs » du TFTP, c'est-à-dire aux analystes du programme, notre parti pris a été de compléter l'analyse des communiqués, des rapports officiels et des écrits d'anciens fonctionnaires publiés depuis 2006. Cette analyse documentaire est enrichie par une série de 15 entretiens réalisée entre 2007 et 2011 auprès de représentants des institutions européennes ayant participé aux négociations de l'accord UE-USA encadrant depuis 2010 le transfert transatlantique de traces financières via le TFTP.

La traçabilité financière comme technique antiterroriste

> 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 penser qu'il s'agit d'un véritable projet de société, poursuivi autant par des pouvoirs privés que par les pouvoirs publics. […] 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 ». (Hermitte, 2003, p. 3)

Les transactions internationales : production et gestion de traces numériques dans un cadre commercial

En tant que technique de gouvernement des hommes et des choses (Torny, 1998), la traçabilité ne relève aucunement d'un monopole d'État et encore moins d'une spécificité liée aux pratiques antiterroristes contemporaines. Les trois éléments de la traçabilité, tels que décomposés par Marie-Angèle Hermitte, sont réunis dans de nombreuses configurations sociales, qu'elles soient commerciales, salariales, sanitaires ou judiciaires pour ne citer que quelques exemples emblématiques. Des recherches menées dans différents champs disciplinaires ont bien montré l'historicité et la multiplicité des usages de traces relatives aux objets et sujets agissants et/ou circulants dans le monde physique ou dans le « cyberespace » (Bonditti, 2007 ; Cochoy, 2002 ; Côté-Boucher, 2009 ; Flichy, 2013 ; Granjou, 2004 ; Gros, 2012 ; Jeandesboz, 2009 ; Mattelart, 2007 ; Pedrot, 2003 ; Razac, 2009 ; Ribaux, 2014 ; Stirling-Belin, 2005).

S'ils peuvent être distingués par les finalités poursuivies, de nombreux systèmes organisés ont en commun de reposer sur la production et l'utilisation de traces numériques comportant des données à caractère personnel, c'est-à-dire des informations permettant d'identifier directement ou indirectement des individus. Certains de ces systèmes portent sur la gestion de circulations, humaines ou non, à l'instar du suivi et de la relocalisation des colis postaux ou des transactions bancaires ; ces deux exemples impliquant des données personnelles sur les expéditeurs et destinataires de ces opérations. Nous privilégions ici la notion de circulation à celle de mobilité car elle « suggère un certain ordre et une certaine organisation des flux, plutôt qu'une mobilité tous azimuts » (D'Aoust, 2014). C'est précisément le cas de l'organisation établie par le principal opérateur mondial de circulation financière, la Society for Worldwide Interbank Telecommunication (ci-après SWIFT), dans le cadre de ses activités commerciales depuis les années 1970.

> Plus de 10 000 établissements financiers et entreprises dans 212 pays nous font confiance au quotidien pour échanger des millions de messages financiers standardisés. […] Nous mettons à disposition la plateforme, les produits et les services de communication internes permettant à nos clients de se mettre en relation et d'échanger des informations financières en toute sécurité et fiabilité. (SWIFT, 2013a, p.1)

Pour filer la métaphore postale (Commission de la protection de la vie privée [CPVP], 2007), SWIFT peut être décrite succinctement comme la principale entreprise d'acheminement et de distribution de « courriers » financiers à travers le monde. En 1973, les représentants de 239 établissements bancaires ont fondé cette coopérative en Belgique afin de se doter collectivement d'une plateforme de communication électronique articulée autour d'un « langage » commun utilisable pour toutes les transactions financières internationales (SWIFT, 2013b). En entamant ce processus de numérisation, il s'agissait de marginaliser progressivement le recours au support papier, au profit d'opérations en ligne, tout en évitant le développement d'initiatives non coordonnées et techniquement incompatibles entre elles. Cela a été chose faite en 1977 avec l'envoi inaugural du premier « message SWIFT ». Entre 1977 et 2013 (année du quarantième anniversaire de la société), SWIFT est passée de moins de quatre millions à plus de quatre milliards de messages traités et distribués par année (SWIFT, 2013b). Dans ce laps de temps, le « code BIC » (*Bank Identifier Code*), plus communément appelé « code SWIFT », est devenu une notion incontournable du langage financier avec 80 % des transactions internationales effectuées à l'aide de ce code (Conseil de l'Union européenne, 2007). Si les produits et services de la compagnie s'adressent aussi aux sociétés de courtage, aux dépositaires centraux de titres ou aux chambres de compensation, l'activité de messagerie demeure principalement dédiée aux opérations interbancaires.

Prenons un exemple concret permettant de saisir la trajectoire d'un message interbancaire, parmi tant d'autres, transitant par SWIFT. Je souhaite effectuer un virement bancaire en direction d'une personne située dans un autre pays et cliente d'une autre banque ou tout du moins d'une autre succursale. Pour ce faire, je passe un ordre de paiement individuel auprès de mon agence ayant recours aux prestations de la coopérative financière. Je n'entre jamais en contact direct avec SWIFT, les employés de ma banque se chargeant de rédiger le message ou courrier financier, c'est-à-dire – pour continuer à filer la métaphore postale – une « lettre » contenue dans une « enveloppe » (l'en-tête du message) (CPVP, 2006).

Sur l'enveloppe sont uniquement indiqués la date et l'heure d'envoi du courrier ainsi que les identifiants des banques impliquées, à commencer par le code BIC. Parmi les éléments qui composent ce fameux code généré par SWIFT, les quatre premiers caractères indiquent le nom

de la banque, les deux suivants précisent son pays d'emplacement, puis deux autres correspondent à sa ville et enfin trois chiffres et/ou lettres viennent spécifier, si besoin, la succursale concernée. Dans l'hypothèse d'un compte ouvert à la Citibank de Toronto au Canada, les huit premiers caractères du code BIC apparaîtraient donc comme suit : CITI CA TT. L'enveloppe ainsi présentée renferme une lettre « cryptée » contenant les précisions nécessaires à la réalisation de mon ordre de paiement. Selon un format standardisé, elle comprend des données permettant de m'identifier et d'identifier le bénéficiaire de ma transaction, à savoir nos noms, numéros de compte bancaire, numéros d'identification nationale, coordonnées postales, téléphoniques et électroniques (Commission européenne, 2013). À cela s'ajoutent des informations complémentaires sur nos banques respectives et, évidemment, sur la somme d'argent à transférer, sur la devise à utiliser et sur la date arrêtée pour réaliser l'opération.

Une fois transmis, le message financier est ramené au statut de trace d'une action désormais révolue et cette trace est préservée pendant 124 jours dans les centres d'exploitation de données administrés par SWIFT (Conseil de l'Union européenne, 2009 ; Groupe de travail « article 29 », 2006). Avec le recueil de ces traces numériques, la coopérative dispose d'une mémoire externe aux acteurs de la transaction afin d'assurer le suivi de ses prestations. Ses employés ont ainsi la possibilité d'aller rechercher les données relatives à chaque opération en cas de litige ou d'informations égarées par leurs clients utilisateurs. On retrouve là un exemple de traçabilité entendue comme « ensemble de techniques qui visent à permettre à tout instant, par des procédés appropriés de constitution de mémoires externes aux personnes, la relocalisation des produits et des marchandises, sans pour autant enfreindre le principe de leur circulation » (Torny, 1998, p. 60). Pour réaliser leur objet social, les représentants de SWIFT ont volontairement organisé la traçabilité des transactions financières internationales. Loin de surgir et d'être laissées par accident, les traces sont ici « provoquées » (Ribaux, 2014) et font partie intégrante de l'environnement financier. Elles sont volontairement générées pour une stratégie définie et conservées pour une durée déterminée avec un mécanisme pour les recueillir et une structure en mesure de les relocaliser et de les analyser aux fins de services après-vente. Les trois éléments de la traçabilité sont ainsi réunis en vue de maîtriser la qualité du service de messagerie et d'instaurer un « cadre de confiance » technico-commercial.

À partir d'octobre 2001, ce système de vigilance a été croisé à un autre effort de traçabilité, toujours concentré sur les mêmes actions mais cette fois-ci au nom d'un tout autre objectif, la lutte contre les « réseaux terroristes ». L'usage renouvelé des traces numériques a alors résulté d'un processus d'hybridation entre des pratiques d'acteurs étatiques et non étatiques esquissant ensemble les contours d'une bureaucratie transnationale de la trace financière. Le TFTP rassemble des éléments émanant de SWIFT, en tant qu'administrateur « privé » de la circulation financière internationale, et du Trésor américain, en tant qu'administrateur « public » de secteurs économiques et financiers.

« Je veux vos données » : vers une bureaucratie hybride et transnationale de la trace financière[2]

Pour évacuer d'emblée toute réflexion illusoire en termes de nouveauté radicale, il convient de noter que l'attention américaine portée aux messages SWIFT à des fins d'enquête et de renseignement n'est pas apparue soudainement après les attentats du 11 septembre 2001. Au tournant des années 1980-1990, une délégation du département de la Justice était d'ores et déjà entrée en contact avec les dirigeants de la coopérative financière (Lichtblau, 2009 ; Zarate, 2013). Sous l'égide de Robert S. Mueller – futur directeur du FBI de septembre 2001 à septembre 2013 –, les membres de cette délégation souhaitaient notamment aboutir à une modification technique du service de messagerie interbancaire. Ils avaient incité leurs interlocuteurs à inclure davantage de données dans les messages distribués et à faciliter leur « décryptage » afin d'être en mesure d'y recourir dans le déroulement d'investigations criminelles. En l'absence de cadre légal contraignant pour appuyer cette demande, ils se virent opposer une fin de non-recevoir. De la même manière, sous l'administration Bush Senior, les agents du « bureau de contrôle des avoirs étrangers » au sein du Trésor (Office of Foreign Assets Control ; ci-après OFAC) tentèrent aussi leur chance, sans plus de succès (Wesseling, De Goede & Amoore, 2012). Régulièrement sollicités dans les années 1990, les dirigeants et les conseillers juridiques de SWIFT ont invariablement répondu par la négative. Leur compagnie au statut particulier n'étant pas assujettie aux obligations anti-blanchiment fissurant le secret bancaire, ils invitaient les autorités américaines à se

2. Co-écrit avec Julien Jeandesboz, un texte à paraître en 2015 proposera une conceptualisation des « bureaucraties hybrides et transnationales des traces numériques ».

tourner directement vers les banques pour obtenir les informations désirées. Ils insistaient également sur leur incapacité technique à accéder aux requêtes individualisées de ces autorités, en raison du « cryptage » des messages SWIFT. Cette situation de blocage a pris fin en octobre 2001 avec la première livraison de traces financières en direction du Trésor.

« Je veux vos données. » Revenant sur la tenue d'une réunion ayant eu lieu dans les locaux du Trésor dans la seconde moitié du mois de septembre 2001, Juan C. Zarate prête ces propos à David Aufhauser en train d'interpeller le directeur général de SWIFT, Leonard Schrank (2013, p. 52). Authentique ou apocryphe, cette phrase rapportée illustre en tout cas avec clarté le principe sur lequel repose encore aujourd'hui le TFTP, celui d'un usage renouvelé de traces numériques produites et conservées par un opérateur de télécommunication.

Deux périodes doivent être distinguées pour bien saisir les modalités pratiques d'accès aux messages SWIFT. De 2001 à 2009, en tant qu'uniques interlocuteurs du Trésor, les représentants de la coopérative financière ont accepté les requêtes émanant du département américain, et plus précisément de l'OFAC, en procédant à l'extraction et à la mise à disposition des messages demandés (Gonzalez Fuster, De Hert & Gutwirth, 2008). Au cours de cette période, la plateforme de communication interbancaire reposait sur deux centres d'exploitation de données, l'un situé dans la ville de Culpeper aux États-Unis et l'autre à Zoeterwoude aux Pays-Bas où tous les messages étaient simultanément archivés durant les 124 jours. Fonctionnant de manière synchrone via un mécanisme de mise en miroir, les deux centres renfermaient effectivement les mêmes traces numériques, celles relatives à l'ensemble des échanges transitant par SWIFT (Conseil de l'Union européenne, 2007 ; Groupe de travail « article 29 », 2006). En adressant exclusivement leurs injonctions au centre américain, les agents du Trésor étaient en mesure d'obtenir la copie de n'importe quel message initié et délivré dans n'importe quel pays et ce, sans aucune forme d'accord préalable avec les responsables des centaines d'États concernés.

On touche ici à la matérialité géographique de la *dataveillance* à grande échelle. Pour être en position de force en matière informationnelle, les acteurs étatiques n'ont pas à contrôler les territoires souverains connectés à des réseaux de communication jugés stratégiques. En revanche, ils doivent s'assurer d'avoir sur leur sol national les sites de stockage des données convoitées ou d'être en mesure de pirater certains

éléments clés de la « machinerie » rendant les communications et leur surveillance possibles, à l'instar des câbles sous-marins (Bauman *et al.*, 2014). En tant que pilier d'un système financier loin d'être complètement déterritorialisé, le fonctionnement de SWIFT dépend d'infrastructures physiques très concentrées géographiquement. Disposer sur son sol de ces infrastructures de communication à vocation mondiale constitue une ressource telle qu'elle déstabilise sensiblement les relations internationales et plus précisément l'égalité formelle entre entités souveraines en matière de gestion et d'échange d'informations (Amicelle, 2013b). C'est précisément cette capacité à transformer unilatéralement l'espace de communication interbancaire en champ d'investigation et à extraire « à la source » les traces des transactions effectuées par des individus et des entreprises à travers le monde qui a suscité la controverse. À la suite des révélations médiatiques sur le TFTP, le programme a été contesté sous l'angle du respect de la vie privée et de la souveraineté économique avec la possibilité d'espionnage des transactions commerciales d'entreprises étrangères. SWIFT étant basée et enregistrée en Belgique, soumise au droit belge et à la législation européenne en matière de protection des données personnelles, le débat a été particulièrement vif en Europe (Parlement européen 2006, 2007, 2009)[3]. Il en a résulté une modification technique de la plateforme de communication financière en 2009 (SWIFT, 2008) et un accord transatlantique en juillet 2010 destiné à encadrer l'accès américain aux messages originaires et/ou à destination de l'Union européenne (Union européenne, 2010).

Sous l'impulsion de ces deux changements s'est ouverte la seconde période de recueil des traces par les agents du Trésor américain travaillant avec leurs homologues d'agences fédérales telles que la CIA. La modification de la plateforme de messagerie financière a eu pour principale conséquence de déconnecter les deux centres historiques de la coopérative avec la création d'un troisième centre opérationnel en Suisse, d'abord provisoirement à Zurich puis définitivement à Diessenhofen. Le centre néerlandais a cessé d'être mis en miroir avec son équivalent américain pour être synchronisé avec ce nouveau centre. De fait, la partie européenne des messages archivés par SWIFT reste

3. « En 2005, par exemple, le volume total de messages traités s'élevait à 2,5 milliards, dont 1,6 milliard pour l'Europe et 467 millions pour les Amériques. Les informations traitées par SWIFT portent sur les messages liés aux transactions financières de centaines de milliers de citoyens européens » (Groupe de travail « article 29 », 2006, p. 8).

dorénavant sur le vieux continent, hors de portée des requêtes adressées au centre de Culpeper. L'accord de cinq ans signé entre l'Union européenne et les États-Unis en 2010 a toutefois pallié cette impossibilité américaine d'accéder directement aux traces numériques stockées exclusivement en Europe. En effet, les agents du Trésor ont toujours la capacité d'effectuer des demandes sur ces messages SWIFT. En contrepartie, le transfert effectif des données ne dépend plus seulement du bon vouloir de la coopérative financière puisque les injonctions du Trésor doivent être préalablement examinées et validées par des agents de l'Office européen de police (Europol). Disposant d'un droit de veto, ils ont pour mission de vérifier que les injonctions du Trésor sont émises dans le respect de l'accord passé et ce, avant toute autorisation de transmission d'informations vers les États-Unis (Europol, 2011). Les représentants du département américain doivent étayer chacune de leurs demandes en explicitant leur légitimité dans un cadre strictement antiterroriste et en justifiant leur portée afin de limiter les volumes de données transférés même si ceux-ci restent considérables, avec plusieurs millions de messages à chaque injonction administrative[4].

Avec ce rôle dévolu à Europol, c'est un marché oligopolistique de l'information financière qui prend forme autour d'un espace transnational de professionnels appartenant à différentes formes d'administration, nationales, supranationales, étatiques et commerciales. Ces relations de pouvoir autour du « Graal » représenté par les centres d'exploitation de données restent à analyser dans toute leur complexité[5]. Toujours est-il qu'une fois extraites d'un de ces centres administrés par SWIFT, les traces couvertes par les demandes américaines sont transférées, stockées et traitées dans une base de données fédérale créée à cet effet sous la responsabilité du Trésor (Commission européenne, 2011 ; U.S. Treasury, 2013a). Les trois éléments de la traçabilité sont reconstitués dans un cadre antiterroriste avec l'articulation des processus de numérisation des communications interbancaires, d'hybridation des pratiques de gestion

4. Il convient de rappeler que le contenu des messages distribués par SWIFT est « crypté ». En référence à ce fait technique, les parties prenantes au TFTP ont argué qu'il leur était impossible de fonctionner à partir de requêtes individualisées visant nominativement les transactions d'une ou plusieurs personnes (U.S. Treasury, 2006, 2007, 2013). L'extraction des messages archivés par SWIFT est réalisée à partir des indications inscrites sur les « enveloppes » (date, heure et identifiants des banques), ceci excluant toute demande fondée sur des noms, des adresses ou des numéros de comptes bancaires spécifiques.

5. Pour un questionnement critique sur le rôle de filtre joué par Europol, voir Amicelle, 2013a.

des traces et de transnationalisation des enjeux de renseignement financier. Il convient désormais d'expliciter et de mettre à l'épreuve les narratifs de légitimation du programme de sécurité nationale.

Des narratifs de légitimation à l'épreuve des « succès » antiterroristes

La justification préemptive

> En réponse à une injonction [administrative], SWIFT met à notre disposition un sous-ensemble de ses archives qu'elle conserve aux États-Unis dans le cadre normal de ses activités commerciales. La base légale de ce type d'injonction est *l'International Emergency Economic Powers Act* (IEEPA), une loi adoptée en 1997 qui permet au gouvernement d'exiger la production d'informations en vertu d'une déclaration présidentielle d'urgence nationale. Nous délivrons de telles injonctions administratives régulièrement, et notre autorité pour le faire est claire. Dans ce cas, nos injonctions sont émises en vertu de la déclaration d'urgence du Président Bush concernant le terrorisme après le 11 septembre 2001 avec l'ordre exécutif 13224 [du 23 septembre 2001]. Cette déclaration a été renouvelée chaque année à la lumière de la menace persistante posée par Al-Qaida et par d'autres groupes terroristes meurtriers. (U.S. Treasury, 2006b, p.2)

Dès octobre 2001, les agents du Trésor se sont prévalus de la promulgation présidentielle d'une situation d'urgence pour recourir à des injonctions administratives (*administrative subpœnas*) afin de recueillir des masses de données transactionnelles auprès de SWIFT et ce, jusqu'à aujourd'hui (U.S. Treasury, 2013a). Ils ont pu collecter les traces numériques souhaitées en contournant les mécanismes balisés du système pénal au nom d'une rapidité d'action présentée comme nécessaire en matière antiterroriste.

En effet, les injonctions administratives diffèrent des ordonnances judiciaires permettant d'obtenir, sous certaines conditions, une grande variété de données dans le cadre d'enquêtes criminelles. Elles dispensent l'enquêteur d'une autorisation judiciaire préalable pour émettre une requête contraignante en direction d'un tiers afin d'accéder aux éléments qu'il estime pertinents. Pour obtenir un mandat de la part d'un magistrat, il y a obligation de faire état de motifs probables (*probable cause*), c'est-à-dire d'éléments devant être jugés suffisants pour croire qu'un délit a été ou est en train d'être commis. Rien de tel avec les injonctions administratives permettant d'agir sur la base d'un soupçon raisonnable,

celui-ci n'ayant pas besoin d'être aussi étayé qu'un motif probable ni d'être validé en amont. Elles se rapprochent en cela de celles émises par un grand jury (*grand jury subpœnas*) en mesure d'exiger la production de documents ou de témoignages sous serment et ce, en pouvant partir d'un simple soupçon. Cependant, une différence majeure existe entre ces deux leviers, avec d'un côté une injonction judiciaire délivrée par un procureur et de l'autre une injonction administrative produite directement par un agent des forces de l'ordre ou affilié, en érigeant le soupçon au-dessus des filtres de la justice criminelle. Véritable clé de voûte du TFTP et d'autres programmes de sécurité, l'usage – récent – des injonctions administratives dans une optique antiterroriste est justifié par l'invocation d'un état de nécessité appelant à la mise en place d'une démarche préemptive.

> Afin d'apprécier l'importance potentielle d'une injonction administrative dans un cas de terrorisme, considérez l'exemple hypothétique suivant. Vendredi après-midi, des enquêteurs du contre-terrorisme apprennent que les membres d'une cellule d'Al-Qaida ont acheté des matériaux destinés à fabriquer une bombe auprès d'une entreprise de produits chimiques. Ils veulent obtenir les documents relatifs à cet achat, documents qui pourraient révéler quel type de produits chimiques a été acheté par les terroristes, ainsi que les documents de livraison qui pourraient révéler la localisation des terroristes. Les enquêteurs contactent un procureur qui délivre une sommation de grand jury pour ces documents. Mais, étant donné que le grand jury n'est pas censé se réunir avant le lundi matin et que le destinataire d'une injonction de grand jury n'est pas tenu de produire les documents avant la prochaine réunion du grand jury, les enquêteurs peuvent ne pas être en mesure d'obtenir les informations pendant trois jours – période durant laquelle la cellule Al-Qaida peut avoir exécuté son plan. Si les enquêteurs avaient l'autorité de délivrer une injonction administrative, ils pourraient obtenir les documents immédiatement et neutraliser la cellule. (U.S. Senate, 2004, pp. 3-4)

Le raisonnement utilitaire régulièrement mobilisé par les représentants de l'administration américaine est ici illustré de manière exemplaire par une figure du département de la Justice. Le pire des scénarios, avec la parabole de la bombe à retardement, fait une nouvelle fois office de ressort argumentatif principal pour justifier l'essor des pratiques antiterroristes en dehors du système pénal et de la logique d'enquête

criminelle[6]. L'utilisation extensive des injonctions administratives est promue en étant adossée à « une approche proactive du terrorisme, reflétant la réalité qu'il n'est pas suffisant de poursuivre les crimes terroristes après leur survenue » (U.S. Senate, 2004, p.2). Paré de ces velléités proactives, le recours à ces injonctions est arrimé à une rationalité préemptive ou pré-crime visant à agir avant que les autres (le ou les suspects et associés) n'agissent[7]. L'imminence et la certitude présumées de l'attaque sont invoquées pour contourner tout ou partie des procédures ordinaires au nom d'une situation extraordinaire dont le caractère provisoire s'éternise.

À l'œuvre sur le plan national, ce contournement des mécanismes habituels de supervision judiciaire en raison de cette nécessité préemptive affirmée est également banalisé à l'international avec le TFTP. Certes, l'accord transatlantique adopté en juillet 2010 encadre l'extraction et le transfert des traces financières conservées en Europe mais d'une manière particulière. Les échanges de données sont réalisés hors des cadres bilatéraux et multilatéraux de référence prévus dans les normes de coopération anti-blanchiment ou les traités d'assistance judiciaire mutuelle (EDPS, 2010). Un tel traité a pourtant été signé en 2003 entre les États-Unis et l'Union européenne. Entré en vigueur en 2010, il favorise le partage d'informations relatives à des comptes et des transactions bancaires aux fins de lutte antiterroriste. De ce point de vue, l'intérêt premier de l'accord transatlantique sur le TFTP réside moins dans le transfert de données *per se* que dans la façon de le faire. Là où la mobilisation des facilités d'entraide judiciaire nécessite la production d'une ordonnance (ou équivalent) associée à la commission d'un crime, le TFTP favorise la mise à disposition purement proactive de l'information sur la base du soupçon, avant même la survenue d'un crime. Certes, l'obtention des traces numériques européennes est désormais soumise à une vérification préalable, mais ce contrôle est effectué selon des modalités étrangères à la supervision judiciaire et à ses garde-fous. La validité des requêtes américaines est évaluée par une agence policière (Europol) « à la lumière de considérations opérationnelles et

6. Pour une discussion critique au sujet de la « bombe à retardement » comme scénario hypothétique justifiant des mesures « exceptionnelles » qui se prolongent dans le temps, voir Delmas-Marty, 2009 et Zedner, 2008.

7. Pour une mise en perspective historique de ce type de rationalité préventive/préemptive afin, encore une fois, de ne pas céder à l'illusion de la nouveauté, voir Finnane et Donkin, 2013.

de besoins en termes de sécurité » (Commission européenne, 2012, p. 7).

Déployé à partir de la justification préemptive, le TFTP est *in fine* valorisé en ce qu'il participe à la production d'une forme de renseignement présentée comme infaillible, le renseignement financier. « La valeur unique du TFTP réside dans l'exactitude de l'information bancaire, dans la mesure où les personnes concernées ont un véritable intérêt à fournir des informations exactes pour s'assurer que l'argent arrive à destination » (Commission européenne, 2013, p. 4).

> Contrairement aux aléas et aux complications du renseignement humain (HUMINT) ou des communications incomplètes et mal interprétées (SIGINT), les empreintes financières ne mentent pas. L'échange d'argent liquide entre opérateurs confirme une connexion ; le virement électronique d'argent dévoile une relation entre détenteurs de comptes ; le transfert d'argent ou de biens entre courtiers identifie des relations d'affaires anciennes. L'enregistrement de ces transactions – adresses, numéros de téléphone, vrais noms, banques utilisées – peut être une mine d'informations. (Zarate, 2013, p. 47)

À cet égard, l'usage « proactif » des messages financiers « décryptés » est systématiquement associé au triptyque « identification, localisation et mise en réseau » (Bruguière, 2010 ; Commission européenne, 2011, 2012, 2013 ; U.S. Treasury 2006a, 2006b, 2007, 2010, 2013a, 2013b).

Identifier, localiser et mettre en réseau : le triptyque officiel du programme de sécurité

« La Commission [européenne] mesurait-elle, lors de la négociation de l'accord [transatlantique sur le TFTP] avec les États-Unis, la différence entre l'extraction de données [*data-mining*] et l'analyse des réseaux sociaux ? » (Parlement européen, 2012, p.1).

Selon l'ensemble des sources disponibles (documents officiels et entretiens), les analystes du TFTP ne sont pas habilités à faire du *data-mining*. Ils ne peuvent s'armer d'algorithmes pour partir librement à la chasse aux traces financières dans la banque de données du Trésor. « Aucune recherche ne peut être menée sur les données tant qu'un enquêteur du TFTP n'a pas fourni des informations préexistantes démontrant un lien entre le sujet de la recherche et le terrorisme ou son financement » (U.S. Treasury, 2013b, p.2). Suivant cette logique, chaque analyste doit faire état d'enquête antiterroriste en cours sur un individu

avant d'être autorisé à lancer le « décryptage » d'un sous-ensemble de traces numériques susceptible de lui être associé. Concrètement, cette démarche préalable consiste surtout à montrer que la personne ciblée est bien répertoriée dans un fichier fédéral de suspects de terrorisme international (Amicelle, 2011) ; 875 000 personnes étaient recensées en 2013 (NCTC, 2013).

À cet égard, les traces financières sont d'abord associées au couple « identification et localisation ». Le « décryptage » et l'usage antiterroriste des messages SWIFT visent à établir leur correspondance avec un suspect connu pour ensuite tenter de le situer territorialement et de suivre ou retracer ses mouvements dans le temps.

> 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. Enfin, même quand un suspect ne change pas de comptes en banque mais bouge en continuant d'utiliser le « vieux » compte (via le e-banking), il a été possible de détecter le changement de localisation, par exemple en identifiant les paiements pour des biens ou des services spécifiques (pour des réparations, ou l'entretien ou d'autres activités habituellement réalisées où une personne vit). […] Même l'« inactivité », en termes de transaction, d'un ou plusieurs comptes bancaires liés à un suspect terroriste est un indicateur utile d'un départ du suspect vers un autre pays. (Commission européenne, 2013, p. 5)

Loin de séparer la traçabilité des hommes et des choses (l'argent dans le cas présent), il y a ici une articulation entre circulation financière et mobilité humaine. Les analystes du TFTP surveillent des mouvements de fonds transitant par SWIFT dans le but affiché de localiser à distance des suspects de terrorisme. Dit autrement, ils partent de la trace numérique des transactions financières pour retrouver la trace physique des individus fichés. La priorité n'est pas, dans un premier temps du moins, de bloquer les flux de capitaux associés à ces individus mais d'appréhender leur circulation comme une ressource en termes de renseignement. Dans cette perspective, loin de s'opposer au principe de libre circulation, les initiatives de sécurité en dépendent.

> Et c'est cette liberté de circulation, au sens large du terme, c'est cette faculté de circulation qu'il faut entendre, je crois, par le mot liberté, et la comprendre comme étant une des faces, un des aspects, une des dimensions de la mise en place des dispositifs de sécurité. (Foucault, 2004, p. 50)

Il y a ensuite une articulation proposée entre connectivité financière et relations humaines. Prendre appui sur la circulation des flux de capitaux et consigner leur trajectoire est promu pour « cartographier les réseaux terroristes de soutien financier, y compris l'identification d'associés inconnus jusqu'alors » (Commission européenne, 2013, p. 6). La métaphore du réseau est d'ailleurs omniprésente dans les écrits officiels sur le TFTP avec une place prépondérante assignée à l'argent en tant que clé de visualisation des « réseaux terroristes ». Comme le souligne de manière critique Marieke de Goede, la connectivité financière est conceptualisée comme la colle ou le liant qui fait tenir le réseau dans son ensemble et c'est en cela qu'elle constituerait une source de renseignement de premier ordre (2012).

> Les traces financières peuvent révéler des liens peu orthodoxes et des relations imprévues dans la mesure où la soif du profit ou le besoin de soutien matériel peut conduire à des mariages de convenance improbables. L'argent est le grand facilitateur et le grand connecteur – même chez les ennemis. Et l'argent ne change de mains que si une relation existe réellement. (Zarate, 2013, p. 48)

L'argent est élevé au rang de dénominateur commun et de grand révélateur des relations humaines. Et plus qu'une simple métaphore, le réseau s'avère être un des principes organisateurs du TFTP. En effet, les agents du programme sont incités à pratiquer l'analyse de réseaux, faisant ainsi écho au « trophée SWIFT » – récompense remise annuellement par la coopérative – dont le mot d'ordre *Linking People Through Technology* semble pris pour argent comptant (SWIFT, 2013b). *De facto*, ces agents doivent travailler sur des réseaux personnels égocentrés puisqu'ils partent d'un « ego », en ayant l'embarras du choix parmi les centaines de milliers de suspects fichés, et se focalisent sur les « nœuds » connectés à cet « ego[8] ». Ils cherchent à établir le réseau entourant le suspect de départ en visualisant ses relations basées sur la circulation de flux financiers.

Cette primauté accordée à la relation financière au travers du TFTP tend à produire une forme de suspicion par association. Avoir envoyé ou reçu de l'argent de la part d'un suspect de terrorisme fait naître le doute si ce n'est le soupçon sur la personne concernée. En cela, la logique de suspicion anime entièrement le TFTP. Elle est à la fois un

8. Pour une présentation synthétique des analyses égocentrées en sciences sociales, voir Marin et Wellman, 2011.

de ses moteurs et son principal résultat puisque les analystes du programme doivent puiser dans un fichier de suspects pour *in fine* l'alimenter en répertoriant les « associés inconnus » des blacklistés (U.S. Treasury, 2006a, 2006b, 2013a, 2013b ; Commission européenne, 2012, 2013). Une importante question de recherche porte sur les modes de qualification des différentes relations et des différents membres des réseaux égocentrés analysés. Être fiché après avoir été payé par un suspect de terrorisme pour « des réparations, ou l'entretien, ou d'autres activités habituellement réalisées où une personne vit » (Commission européenne, 2013, p. 5) semble un peu court… Sur quels critères les agents du TFTP discriminent-ils les relations pertinentes et dans quelle mesure poursuivent-ils l'analyse vers les relations des relations des suspects connus et ainsi de suite ? À titre de comparaison, les documents divulgués par Edward Snowden sur divers programmes de surveillance initiés sous l'égide de la National Security Agency américaine (ci-après NSA) font état d'une logique de suspicion poussée jusqu'à trois degrés de séparation.

> Autrement dit, pour un suspect ayant 100 amis au premier degré, l'individu chargée de la surveillance à la NSA ou au sein d'un de ses sous-traitants privés peut, sans mandat, mettre sous surveillance l'ensemble des 2 669 556 connexions potentielles au troisième degré. (Bauman *et al.*, 2014, p. 125)

Le paradoxe des exemples de réussite

Si les contours de la logique de suspicion demeurent flous au regard des informations disponibles, l'efficace antiterroriste de la justification préemptive est encore moins claire. Alors que cette justification a permis aux agents du Trésor d'extraire les pratiques d'échange de données personnelles du système pénal et de la supervision judiciaire, sa traduction opérationnelle mérite d'être interrogée à la lumière des « succès » rendus publics.

En décembre 2012 et en novembre 2013, une série de cas a été publiée dans deux rapports d'inspection UE-USA du TFTP pour donner matière aux déclarations répétées sur la valeur ajoutée du programme. Or, l'écrasante majorité de ces exemples porte sur des usages de messages SWIFT dans le cadre d'investigations menées après la commission d'un crime violent, pas avant. Qui plus est, la dimension

préemptive du programme est précisément mobilisée en référence à une de ces enquêtes lancées après un attentat, celui ou plutôt ceux perpétrés par Anders Behring Breivik en Norvège le 22 juillet 2011.

> Europol et les États membres sont de plus en plus conscients de la valeur des données du TFTP dans leur tâche pour combattre et prévenir le terrorisme et son financement dans l'Union européenne. Un exemple particulièrement frappant examiné lors de l'inspection est le cas Breivik pour lequel des informations relevant du TFTP ont aidé les Norvégiens et les autres enquêteurs européens, incluant Europol, à identifier en quelques heures les circuits par lesquels Breivik a collecté et déplacé les fonds qu'il a utilisés pour la préparation de ces attaques barbares. Plus des connaissances sont acquises sur les comportements financiers de ce type de terroristes (« loups solitaires »), mieux sont préparées les forces de l'ordre et les autres autorités à comprendre la façon de penser de ces individus et en définitive à prévenir des attaques similaires. À partir des données du TFTP collectées dans le contexte du cas Breivik, les autorités finlandaises ont été en mesure d'arrêter une personne poursuivant des objectifs terroristes similaires avant que cette personne ne puisse les mettre en œuvre. (Commission européenne, 2012, pp. 14-15)

L'accent mis sur cet exemple pour justifier de la pertinence du TFTP est pour le moins paradoxal. Censé illustrer la plus-value et donc la légitimité du programme vis-à-vis des dispositifs existants, le cas Breivik tend plutôt à démontrer l'inverse.

Loin de l'argumentaire récurrent autour du triptyque « identifier, localiser et mettre en réseau », le TFTP est ici convoqué pour des pratiques de profilage visant à définir le comportement financier d'un criminel dans le but de détecter par la suite des profils similaires. Or, sans avoir attendu la création du TFTP, la mise en œuvre de ce type de pratiques, aux résultats par ailleurs controversés, était déjà banalisée dans le cadre des autres dispositifs de lutte contre le blanchiment d'argent et le financement du terrorisme (Amicelle & Favarel-Garrigues, 2009 ; Verhage, 2011). De surcroît, à moins de considérer que « des attaques similaires » sont effectivement imminentes et certaines, la justification préemptive du recours proactif aux injonctions administratives peut être discutée. D'autant que l'utilité du TFTP n'est pas non plus démontrée dans l'accès aux traces financières d'Anders Behring Breivik, nécessaires pour en extraire le profil. Suivant une logique classique d'enquête criminelle, l'investigation a débuté après que Breivik a commis ses crimes, pas avant, ce qui signifie que l'usage du TFTP

était tourné vers un événement ayant déjà eu lieu. À ce titre, l'utilisation des mécanismes existants en matière d'entraide judiciaire internationale ou de coopération anti-blanchiment aurait permis d'aboutir aux mêmes renseignements financiers. À partir d'un cas érigé en modèle d'efficacité, les bénéfices opérationnels du TFTP apparaissent bien moins tangibles que ses conséquences sur l'encadrement des pratiques transnationales de *dataveillance* financière.

Enfin, la qualité des traces numériques et à travers elles le statut donné au renseignement financier devraient aussi être davantage interrogés. La matière première travaillée par les analystes du TFTP se résume aux codes BIC tamponnés sur les enveloppes des centaines de millions de « courriers » collectés. Si l'exactitude de ces codes est évidente puisqu'elle conditionne la réalisation des transactions, on ne peut en dire autant pour le contenu des messages SWIFT. Les acteurs bancaires commettent régulièrement des petites fautes dans le corps de ces messages, que ce soit dans la transcription des noms, des adresses ou des numéros d'identification nationale. Au regard du nombre de communications à passer quotidiennement sans ralentir la fluidité des flux financiers, ils s'en accommodent volontiers à partir du moment où les données disponibles, bien qu'imparfaites, leur suffisent à authentifier et à acheminer le courrier. Alors que cette marge d'erreur est – jusqu'à un certain point – tolérable et sans conséquence pour l'organisation de la circulation financière, elle s'avère être plus problématique pour la production de renseignement financier. La différence entre Anthony Amicelle et Antony Amicel peut sembler minime, voire insignifiante dans un contexte d'action mais considérable dans un autre, en particulier pour les prénoms et patronymes très répandus accentuant la difficulté avec des cas d'homonymie. Il s'agit là d'un point encore trop souvent négligé par les parties prenantes aux discussions sur les pratiques antiterroristes et les programmes de *dataveillance* à grande échelle. Que ce soit pour promouvoir une société plus sûre ou pour s'insurger contre une société de surveillance, les défenseurs comme les détracteurs de ces initiatives partagent souvent les mêmes certitudes sur les capacités des technologies en place. Or ces capacités – rassurantes ou effrayantes – sont intrinsèquement limitées et sujettes à des défaillances, en raison notamment de la qualité aléatoire des traces numériques à traiter. À ce titre, postuler que les traces financières « ne mentent pas » est une affirmation abusive.

Conclusion

Fondé sur un espace hybride de relations et de pratiques à la fois au-dessus, au-delà et en deçà du national, le TFTP participe à la production de renseignement financier à partir d'un dispositif transnational de traçabilité des flux de capitaux. Plutôt que de terminer cet article en résumant ses idées-forces, nous souhaitons conclure en proposant trois hypothèses exploratoires pour répondre à la question qui émerge à la suite de notre développement. Si, à la lumière des sources disponibles, les résultats concrets de ce programme de sécurité ne coïncident manifestement pas avec les éléments dont il tire sa légitimité, pourquoi perdure-t-il après plus de dix ans de fonctionnement ?

En apprenant l'existence du TFTP par voie de presse en 2006, les députés du Parlement européen et les représentants des autorités européennes de protection des données avaient formulé l'hypothèse d'un usage multitâche des traces financières collectées. Émettant des doutes sur la finalité strictement antiterroriste du programme, ils avaient fait part de leur crainte en matière d'espionnage économique et industriel. Au-delà des atteintes aux droits fondamentaux des citoyens de l'Union européenne, ils s'étaient émus de l'accès potentiel de l'administration américaine à des informations stratégiques sur des transactions financières et des opérations commerciales impliquant les entreprises des États membres de l'UE. Malgré les démentis apportés par les représentants des États-Unis, le sujet a été régulièrement remis sur le métier jusqu'à la signature de l'accord transatlantique de 2010 venant formellement encadrer la collecte et le traitement des traces financières conservées en Europe. Contrairement aux divulgations sur les programmes de la NSA, aucune pratique d'espionnage économique ou politique n'a été démontrée concernant le TFTP.

Deuxièmement, il convient de saisir l'importance du programme et de sa base de données pour le département du Trésor en termes de « capital symbolique » dans les relations de pouvoir qui structurent le domaine de la sécurité nationale[9]. Le TFTP est effectivement appréhendé comme une ressource par et pour des acteurs en quête de reconnaissance dans un espace social spécifique. Pensée dès le début ou rationalisée *a posteriori*, cette dimension a été clairement explicitée.

9. Pour une réflexion sur le capital symbolique et informationnel représenté par les bases de données dans l'espace de relations entre les agences de sécurité européennes, voir Bigo, 2013.

Ainsi, à propos de son ouvrage accordant une place de choix au TFTP, Juan C. Zarate précise que :

> c'est aussi l'histoire d'un petit groupe de fonctionnaires venant du département du Trésor et d'autres agences gouvernementales qui ont modelé cette nouvelle forme de pouvoir financier. Ces stratégies ont été préparées en toute discrétion, avec la mission de réorganiser la façon dont les outils financiers étaient utilisés. Elles ont aussi servi à ressusciter un département du Trésor qui luttait pour rester pertinent sur les enjeux de sécurité nationale. […] Nous imaginions un jour où le département du Trésor deviendrait central pour les questions essentielles en sécurité nationale, et c'est exactement ce qui est arrivé. (2013, p. xi)

Le fait que les agents de la NSA aient tenté de pirater les serveurs du nouveau centre de SWIFT en Suisse, pour accéder directement aux messages financiers sans passer par le Trésor, incite à creuser cette hypothèse sur le renseignement financier comme enjeu de lutte entre agences fédérales (Parlement européen, 2013 ; Schmuck, 2013).

Enfin, dans la continuité du point précédent, le TFTP – comme d'autres programmes américains mais aussi européens de *dataveillance* à grande échelle – pose avec acuité la « question informationnelle » en relations internationales. Cette question renvoie aux « écarts de pouvoir qui résultent de la distribution différentielle de stocks d'informations ou, du moins, des inégalités d'accès à des dispositifs de production d'informations » (Linhardt, 2005, p. 259). S'il a quelque peu rééquilibré le rapport de force entre les États-Unis et l'Union européenne, l'accord transatlantique de 2010 a surtout entériné le caractère profondément asymétrique des relations entre l'administration américaine et les quelque 180 autres États hors UE connectés au réseau SWIFT. Avec l'usage banalisé des injonctions administratives, les agents du Trésor détiennent des informations sur des millions de personnes issues de pays tiers sans dépendre de l'aval de leurs administrations nationales ou être contraints par leur cadre législatif. Cette forme d'inégalité que traduit et reproduit le TFTP entre entités souveraines est d'ailleurs reconnue et en partie valorisée.

> Basé sur le TFTP, il a été possible d'obtenir des informations sur des citoyens et des résidents américains et européens suspectés de terrorisme ou de financement du terrorisme dans des pays tiers où les demandes d'assistance judiciaire mutuelle ne sont pas traitées en temps voulu. (Commission européenne, 2013, p.6)

Le programme permet ainsi à ces utilisateurs et bénéficiaires de s'affranchir des contingences étrangères en matière de sécurité et de renseignement, que ce soit les aléas diplomatiques ou les difficultés d'ordre technique, relationnel et opérationnel. Cet élément semble contribuer fortement à la pérennisation du TFTP.

Sans épuiser les possibilités de compréhension des dynamiques sociales, politiques et économiques à l'œuvre, ces hypothèses non mutuellement exclusives invitent à travailler l'objet de recherche « renseignement financier » sous l'angle des rapports de domination qu'il suscite.

Références

Amicelle, A. (2011). The Great (data) bank robbery : The Terrorist Finance Tracking Program & the SWIFT affair. *Questions de recherche / Research Questions*, *36*, 1-27.

Amicelle, A. (2013a). The EU's paradoxical efforts at tracking the financing of terrorism. From criticism to imitation of dataveillance. *CEPS Liberty and Security Series*, *56*, 1-19.

Amicelle, A. (2013b). Les professionnels de la surveillance financière. *Criminologie*, *46* (2), 195-219.

Amicelle, A., & Favarel-Garrigues, G. (2009). La lutte contre l'argent sale au prisme des libertés fondamentales : Quelles mobilisations ? *Cultures & Conflits*, *76*, 39-66.

Aufhauser, D. (2003). Terrorist financing : foxes run to ground. *Journal of Money Laundering Control*, *6* (4), 301-305.

Bauman, Z., Bigo, D. Esteves, P, Guild, E., Jabri, V, Lyon, D., & Walker, R. J. B. (2014). After Snowden : Rethinking the impact of surveillance. *International Political Sociology*, *8*, 121-144.

Bigo, D. (2013). The transnational field of computerised exchange of information in police matters and its european guilds. Dans N. Kauppi & M. Rask Madsen (Eds.), *Transnational Power Elites : The new professionals of governance, law and security* (pp. 155-182). London : Routledge.

Bigo, D, Boulet, G., Bowden, C., Carrera, S., Guild, E., Hernanz, N., De Hert, P., Jeandesboz, J., & Scherrer, A. (2013). Open season for data fishing on the Web : The challenges of the US PRISM programme for the EU. *CEPS Policy Briefs*, *293*, 1-10.

Bonditti, P. (2008). *L'antiterrorisme aux Etats-Unis (1946-2007) : une analyse foucaldienne de la transformation de l'exercice de la souveraineté et de l'art de gouverner* (Thèse de doctorat). Paris : Sciences Po Paris.

Bruguière, J.-L. (2010). *Second report on the processing of EU-originating personal data by the United-States Treasury Departement for Counter Terrorism purposes : Terrorist Finance Tracking Program*. Brussels.

Cassara, J., & Jorisch, A. (2010). *On the trail of terror finance : What law enforcement and intelligence officers need to know.* Arlington, VA : Red Cell Intelligence Group.

Cochoy, F. (2002). Une petite histoire du client, ou la progressive normalisation du marché et de l'organisation. *Sciences de la société, 44*(3), 357-380.

Côté-Boucher, K. (2009). Interdictions à la mobilité, identités autorisées et échange de renseignements : La frontière intelligente vue du Canada. Dans A. Sherrer, E.-P. Guittet & D. Bigo (Eds.), *Mobilités sous surveillance. Perspectives croisées UE-Canada* (pp. 129-147). Montréal : Athéna Éditions.

Commission de protection de la vie privée [CPVP]. (2006). *Avis n°37 relatif à la transmission de données à caractère personnel par la SCRL SWIFT suite aux sommations de l'UST (OFAC).* Bruxelles.

Commission de protection de la vie privée [CPVP]. (2007). *Dossier Technique. Affaire SWIFT.* Bruxelles.

Commission européenne. (2011). *Commission report on the joint review of the implementation of the agreement between the European Union and the United States of America on the processing and transfer of financial messaging data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program.* Brussels.

Commission européenne. (2012). *Commission Staff Working Document – Report on the second joint review of the implementation of the Agreement between the European Union and the United States of America.* Brussels.

Commission européenne. (2013). *Joint Report from the Commission and the U.S. Treasury Department regarding the value of TFTP Provided Data.* Brussels.

Conseil de l'Union européenne. (2007). *Processing and protection of personal data subpoenaed by the Treasury Department from the US based operation centre of the Society for Worldwide Interbank Financial Telecommunication (SWIFT).* Luxembourg, 11291/07.

Conseil de l'Union européenne. (2009). *Information Note : EU-US agreement on the processing and transfer of financial messaging data for purposes of the US Terrorist Finance Tracking Program (TFTP).* Brussels.

D'Aoust, A.-M. (2014). *Transports : Penser la circulation et la sécurité.* Descriptif présenté au colloque organisé à l'Université du Québec à Montréal.

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

Delmas-Marty, M. (2009). Liberté et sûreté : les mutations de l'état de droit. *Revue de synthèse, 130*(3), 465-491.

European Data Protection Supervisor [EDPS]. (2007). *EDPS opinion on the role of the European Central Bank in the SWIFT case.* Brussels.

Europol. (2011). *Terrorist finance tracking programme (TFTP) – The EU-US TFTP Agreement. Questions and Answers.* The Hague.

Favarel-Garrigues, G. (2003). L'évolution de la lutte anti-blanchiment depuis le 11 septembre 2001. *Critique internationale, 20*, 37-46.

Finnane, M., & Donkin, S. (2013). Fighting terror with law? Some other genealogies of pre-emption. *International Journal for Crime and Justice, 2* (1), 3-17.

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

Foucault, M. (2004). *Sécurité, territoire, population. Cours au Collège de France 1977-1978*. Paris : Éditions Seuil/Gallimard.

Gonzalez Fuster, G., De Hert, P., & Gutwirth, S. (2008). SWIFT and the vulnerability of transatlantic data transfers. *International Review of Law Computers & Technology, 22*(1-2), 191-202.

Granjou, C. (2004). La traçabilité, un dispositif de confiance dans les activités techniques. L'exemple de la filière viande bovine. *Cahiers internationaux de sociologie, 115*, 327-342.

Gros, F. (2012). *Le principe sécurité*. Paris : Éditions Gallimard.

Groupe de travail « article 29 ». (2006). *Opinion 10/2006 on the processing of personal data by the society for Worldwide Interbank Financial Telecommunication (SWIFT)*. Brussels.

Guittet, E.-P. (2006). « Ne pas leur faire confiance serait leur faire offense ». Antiterrorisme, solidarité démocratique et identité politique. *Cultures & Conflits, 61*, 51-76.

Hermitte, M.-A. (2003). La traçabilité des personnes et des choses. Précaution, pouvoirs et maîtrise. Dans P. Pedrot (Ed.), *Traçabilité et responsabilité* (pp. 1-44). Paris : Economica.

Jeandesboz, J. (2009). Logiques et pratiques de contrôle et de surveillance des frontières de l'Union européenne. Dans A. Sherrer, E.-P. Guittet & D. Bigo (Eds.), *Mobilités sous surveillance. Perspectives croisées UE-Canada* (pp. 129-147). Montréal : Athéna Éditions.

Levi, M. (2010). Combating the financing of terrorism. A history and assessment of the control of "threat finance". *British Journal of Criminology, 50* (4), 650-669.

Lichtblau, E. (2009). *Bush's law. The remaking of American justice*. New York, NY : First Anchor Books Edition.

Lichtblau, E., & Risen, J. (2006, 23 juin). Bank data sifted in secret by U.S. to block terror. *The New York Times*. Repéré à http://www.nytimes.com/2006/06/23/washington/23intel.html?pagewanted=all&_r=0.

Linhardt, D. (2005). La « question informationnelle ». Éléments pour une sociologie politique des fichiers de police et de population en Allemagne et en France. *Déviance et Société, 29*, 259-272.

Marin, A., & Wellman, H. (2011). Social network analysis : an introduction. Dans P. Carrington & J. Scott (Eds.), *The Sage Handbook of social network analysis* (pp. 11-25). London : Sage.

Mattelart, A. (2008). *La globalisation de la surveillance. Aux origines de l'ordre sécuritaire*. Paris : Éditions La Découverte.

National Counterterrorism Center [NCTC]. (2013). *A counterterrorism center of gravity. Overview*. Washington D. C.

Parlement européen. (2006). *Résolution du Parlement européen sur l'interception des données des virements bancaires du système SWIFT par les services secrets américains.* Strasbourg.

Parlement européen. (2007). *Résolution du Parlement européen sur SWIFT, l'accord PNR et le dialogue transatlantique sur ces questions.* Bruxelles.

Parlement européen. (2009). *Résolution du Parlement européen sur l'accord international envisagé pour mettre à la disposition du département du Trésor des États-Unis des données de messagerie financière afin de prévenir et de combattre le terrorisme et le financement du terrorisme.* Bruxelles.

Parlement européen. (2012). *Parliamentary questions. Subject : Implementation of the EU-US Terrorist Finance Tracking Programme Agreement* (O-000175/2012). Brussels.

Parlement européen. (2013). *Communiqué de presse. Le Parlement demande la suspension de l'accord UE-États-Unis sur les données bancaires suite à l'espionnage de la NSA*. Bruxelles.

Pedrot, P. (2003). *Traçabilité et responsabilité.* Paris : Economica.

Razac, O. (2009). *Histoire politique du barbelé.* Paris : Editions Flammarion.

Ribaux, O. (2014). *Police scientifique. Le renseignement par la trace.* Lausanne : Presses polytechniques et universitaires romandes.

Schmuck, P. (2013, 12 septembre). Pourquoi la NSA a espionné un village thurgovien. *Le Matin*. Repéré à http://www.lematin.ch/suisse/Pourquoi-la-NSA-a-espionne-un-village-thurgovien-/story/18340039.

Sheptycki, J. (2000). Policing the virtual launderette : Money laundering and global governance, Dans J. Sheptycki (Ed.), *Issues in Transnational Policing* (pp. 135-176). New York : Routeledge.

Stirling-Belin, F. (2005). Traçabilité, liberté de circulation et Union européenne. *Revue de la recherche juridique, droit prospectif, 30*(1), 409-432.

SWIFT. (2008). *Distributed Architecture : Allocation of Countries to the Two Messaging Zones.*

SWIFT. (2013a). *Informations sur l'entreprise.*

SWIFT. (2013b). *Historique de SWIFT.*

Taylor, J. B. (2008). *Global financial warriors. The untold story of international finance in the post 9/11 world*. New York : W. W. Norton.

Torny, D. (1998). La traçabilité comme technique de gouvernement des hommes et des choses. *Politix*, *44*, 51-75.

Union européenne. (2010). *Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program* (OJ 2010, L 195/5). Brussels.

U.S. Senate Judiciary Committee. Subcommittee on Terrorism, Technology and Homeland Security. (2004). *Tools to Fight Terrorism : Subpoena Authority and Pretrial Detention of Terrorists. Testimony of the Principal Deputy Assistant Attorney General, Office of Legal Policy, U.S. Department of Justice.* Washington D.C.

U.S. Treasury. (2006a). *Terrorist Finance Tracking Program – Factsheet*. Washington D.C.

U.S. Treasury. (2006b). *Testimony of Stuart Levey, Under Secretary, Terrorism and Financial Intelligence, US Department of the Treasury, Before the House Financial Services Subcommittee on Oversight and Investigations*. Washington D.C.

U.S. Treasury. (2007). *Lettre du département du Trésor des États-Unis concernant SWIFT/programme de surveillance du financement du terrorisme*. JO, C 166/17.

U.S. Treasury. (2010). *Terrorist Finance Tracking Program – Factsheet*. Washington D.C.

U.S. Treasury. (2013a). *Resource Center : Terrorist Finance Tracking Program (TFTP)*. Washington D.C.

U.S. Treasury. (2013b). *Terrorist Finance Tracking Program (TFTP) : Questions & Answers*. Washington D.C.

Verhage, A. (2011). *The anti-money laundering complex and the compliance industry*. New York : Routledge.

Vlcek, W. (2008). A leviathan rejuvenated : Surveillance, money Laundering, and the War on Terror. *International Journal of Politics, Culture and Society*, *20*(1-4), 21-40.

Wesseling, M., De Goede, M., & Amoore, L. (2012). Data wars beyond surveillance : Opening the black box of SWIFT", *Journal of Cultural Economy*, *5*(1), 49-66.

Zarate, J. C. (2013). *Treasury's war. The unleashing of a new era of financial warfare*. New York : Public Affairs.

Zedner, L. (2008). Terrorism, the ticking bomb and criminal justice. *Criminal Justice Matters*, *73*(1), 18-19.

ABSTRACT • *The paper deals with an issue that is understudied despite its growing importance for the field of transnational policing, namely financial intelligence. In order to contribute to the reflection on this key component of surveillance practices – or rather dataveillance – the analysis focuses more precisely on the American Terrorist Finance Tracking Program (TFTP). Based on a set of relations above, beyond and below the national, this security program contributes to the production of intelligence from a traceability apparatus of financial transactions. The paper aims to explain the conditions for the existence of such a mechanism, which consists of mobilizing large quantities of digital traces generated by a particular form of cross-border transaction. It also aims to challenge the legitimacy of the TFTP in terms of its justification and its 'successes'.*

KEYWORDS • *Financial intelligence, traceability, surveillance, national security, anti-terrorism.*

RESUMEN • *El presente artículo esta consagrado a un tema todavía poco estudiado a pesar de su importancia creciente en un área como la del* policing *transnacional, a saber : la inteligencia financiera. Con el fin de contribuir a la reflexión sobre este componente de las prácticas contemporáneas de vigilancia, o más bien de "datavigilancia", el análisis trata, más precisamente, del programa americano de acecho al*

*financiamiento del terrorismo (*Terrorist Finance Tracking Program [TFTP]-*en inglés-)*. *Fundado en un espacio de relaciones, a la vez sobre, más allá, y en continuación con el nacional, este programa de seguridad participa en la producción de vigilancia a partir de un dispositivo de rastreo de flujos financieros. Así, se intenta explicitar las condiciones de existencia de dicho dispositivo, que consiste en la movilización de grandes conjuntos de huellas informáticas generadas por una forma particular de circulación transfronteriza. Aquí se trata, también, de poner a prueba la legitimidad del TFTP frente a la justificación narrativa y a los "éxitos" que le son atribuidos.*

PALABRAS CLAVE • *Inteligencia financiera, rastreo, vigilancia, seguridad nacional, antiterrorismo.*