“ Nous ne sommes pas un Big Brother ! ” Autorité et stratégies de légitimation des services de renseignement dans la captation et l’usage des données numériques

Didier Bigo, Laurent Bonelli

Cultures & Conflits

114-115 | été/automne 2019
Les mondes du renseignement entre légitimation et contestation

« Nous ne sommes pas un Big Brother ! »

Autorité et stratégies de légitimation des services de renseignement dans la captation et l'usage des données numériques

"We aren't a Big Brother!" The Authority and Legitimization Strategies of Intelligence Services in the Capture and Use of Digital Data

Didier Bigo et Laurent Bonelli

Édition électronique
URL : http://journals.openedition.org/conflits/21180
DOI : 10.4000/conflits.21180
ISSN : 1777-5345

Éditeur :
CCLS - Centre d'études sur les conflits lilberté et sécurité, L'Harmattan

Édition imprimée
Date de publication : 20 décembre 2019
Pagination : 199-226
ISBN : 978-2-343-19249-9
ISSN : 1157-996X

Distribution électronique Cairn

Référence électronique
Didier Bigo et Laurent Bonelli, « « Nous ne sommes pas un Big Brother ! » », *Cultures & Conflits* [En ligne], 114-115 | été/automne 2019, mis en ligne le 01 janvier 2023, consulté le 16 janvier 2020. URL : http://journals.openedition.org/conflits/21180 ; DOI : 10.4000/conflits.21180

« Nous ne sommes pas un Big Brother ! »

Autorité et stratégies de légitimation des services de renseignement dans la captation et l'usage des données numériques

Didier BIGO, Laurent BONELLI

Didier Bigo est professeur de Sociologie Politique Internationale (IPS) à Sciences Po Paris et Research professor, Department of war Studies, King's College London. Il est Directeur du Centre d'études sur les Conflits, la Liberté, la Sécurité (CCLS) ainsi que co-rédacteur en chef de Cultures & Conflits *et de* PARISS.

Laurent Bonelli est maître de conférences en science politique à l'université de Paris-Nanterre et membre de l'Institut des Sciences sociales du Politique (UMR CNRS 7220). Il est co-rédacteur en chef de Cultures & Conflits *et Associate Editor de* International Political Sociology.

Des interceptions à grande échelle réalisées par la *National Security Agency* (NSA) américaine – et révélées en 2013 par Edward Snowden – à la surveillance assidue des réseaux sociaux utilisés par les Gilets jaunes, en passant par la reconstitution des échanges entre partisans de groupes armés se réclamant du « djihadisme », les données numériques sont à l'évidence devenues un enjeu et un objet central du travail des services de renseignement.

Ce simple constat a ouvert un large débat politique, juridique, philosophique et académique sur les relations entre le contrôle des opinions, des mobilités et des communications et la croissance exponentielle des traces laissées par les activités quotidiennes des individus usant des technologies numériques, qu'elles soient publiques ou pas. Que sont ces traces, qu'enregistrent-elles et comment ? Sont-elles des « données brutes » à disposition de tous ou relèvent-elles de la vie privée ? À qui appartiennent les données ? Comment sont-elles constituées en nouvelles sources d'enrichissement, de profits commerciaux, de savoir statistique sur les populations, de connaissance de l'intimité des individus, et bien sûr de surveillance ?

La transformation des activités et des comportements *on-line* des individus en données, grâce à des mécanismes automatisés de collecte et d'exploitation, a été pensée par des acteurs commerciaux d'Internet comme une contrepartie de la « gratuité » des services qu'ils leur offrent [1]. Mais cette expansion inégalée des traces numériques a été également vue par les organisations intéressées au renseignement au sens large – policiers, militaires, agents d'immigration ou des finances, douaniers – comme une opportunité extraordinaire pour produire des savoirs approfondis sur les pratiques individuelles, qui ne pouvait pas rester entre les mains du secteur privé. Se défendant d'être « un Big Brother » orwellien [2], la plupart de ces professionnels intègrent désormais le recueil de données personnelles venant de multiples secteurs de la vie sociale d'un individu et de ses relations, ainsi que leur analyse dans leur activité. Mais ils le font de manière diverse selon leur ancienneté dans le métier, leurs capacités en termes de personnel, de moyens financiers et technologiques, et surtout selon leurs visions de ce qu'est l'activité de renseignement. Ceux qui pensent le renseignement dans les catégories de la lutte contre le criminel et de la recherche de preuves, ceux qui le voient comme une activité secrète allant de l'espionnage jusqu'aux éliminations physiques mais qui se justifient par des impératifs de sécurité nationale et ceux qui cherchent à identifier des suspects inconnus en essayant – *via* des algorithmes – de détecter des anomalies de comportement afin de déterminer des profils de risque, n'ont ainsi pas suivi la même voie ni développé le même usage des informations numériques.

Ces différents acteurs ont discuté, entre eux puis avec les gouvernants, de la valeur de ces données, de leur accumulation et de leur mise en relation par des logiciels. La question s'est posée de l'utilité d'engager des moyens financiers et humains importants pour l'acquisition de techniques d'interception à distance (satellitaire, numérique) et de leur avantage relatif par rapport aux alternatives pour obtenir les mêmes résultats *via* des techniques *undercover* ou des informateurs. Chacun a répondu de manière assez différente, en fonction de la position qu'il occupe dans le champ des professionnels de la sécurité. Si tous se sont bien rendu compte de la facilité d'accumuler, d'échanger et de conserver ces données, jusqu'où leur accumulation n'était-elle pas contre-productive, multipliant les détails mais perdant en route les grandes lignes ? Les services les plus spécialisés n'ont pas toujours été convaincus par l'accumulation (*collect it all*) et ont préféré garder leurs dossiers les plus sensibles hors des circuits de collecte et d'échange, qui se sont en revanche multipliés pour des allégations de suspicion peu fondées [3]. L'irruption de controverses

1 . Manokha I., « Le scandale Cambridge Analytica contextualisé : le capital de plateforme, la surveillance et les données comme nouvelle "marchandise fictive" », *Cultures & Conflits*, n°109, 2018, pp. 39-59.

2 . Voir par exemple l'article de Bernard Bajolet, alors directeur général de la sécurité extérieure française, « La DGSE, outil de réduction de l'incertitude ? », *Revue Défense Nationale*, janvier 2014, n°766, pp. 27-31.

3 . Bigo D. « Shared Secrecy in a Digital Age and a Transnational World », *Intelligence and National Security*, vol. 34, n°3, 2019, pp. 379-94.

publiques à la suite de divulgation des pratiques de violation des droits de l'homme par la *Central Intelligence Agency* (CIA) et ses complices, puis de l'interception à grande échelle de données personnelles par la NSA et les *Five Eyes*, ainsi que celles de l'usage régulier de drones hors des zones de guerre, ont obligé chacun des grands services à revoir l'intérêt de ces techniques, au regard non seulement des enjeux de sécurité, mais aussi en raison des limites imposées par les règles judiciaires et celles de la vie privée et plus généralement des contraintes inhérentes à un espace qui se veut démocratique [4].

Dans cet article, nous n'allons pas étudier l'ensemble des professionnels de la sécurité. Nous nous limiterons aux principaux services de renseignement de neuf pays occidentaux (États-Unis, Grande Bretagne, Canada, Australie, Nouvelle Zélande, France, Allemagne, Espagne et Suède), identifiés à partir de la littérature existante et des travaux mentionnant les formes les plus fréquentes de collaboration internationale. Il s'agit de services qui ont les capacités et l'autorité d'intercepter les données non seulement chez eux, mais aussi à l'étranger. Ils sont pour la plupart ceux des anciennes puissances coloniales, qui considèrent avoir un rôle à jouer à une échelle régionale ou globale. L'espace transnational qu'ils forment est lié d'une part à l'histoire des alliances durant la Seconde Guerre mondiale entre démocraties et plus récemment à ceux qui ont réussi à jouer un rôle majeur dans la géopolitique des câbles internet. On a appelé cet espace par le nom d'un de leur groupement spécialisé dans la surveillance des communications : les *Five Eyes*, ou les *Five Eyes Plus*, mais cet espace ne se réduit pas à ces seuls services comme nous allons le voir. L'histoire de cette alliance est connue et se réduit souvent à celle d'une sensibilité commune entre services d'origine anglo-saxonne qui aurait créé les conditions d'une confiance réciproque. Ce récit historico-culturaliste ne résiste toutefois pas à l'analyse [5]. Il faut au contraire étudier les moyens et pratiques des services pour les distribuer dans un espace transnational, sans présupposer qu'une appartenance nationale les soumettrait par défaut à une proximité de positions. S'inspirant des travaux de Pierre Bourdieu [6], cet article se propose de systématiser les éléments recueillis lors d'entretiens menés entre

4 . Bigo D., « Security, surveillance and democracy » in Ball K., Lyon D. (dir.), *Routledge Handbook of Surveillance Studies*, Routledge, Londres, 2012 ; « Digital surveillance and everyday democracy », in Weber L., Fishwick E. et M. Marmo (dir.), *The Routledge International Handbook of Criminology and Human Rights*, Routledge, Londres, 2016 ; Guild E., Bigo D. et M. Gibney (dir.), *Extraordinary Rendition: Addressing the Challenges of Accountability*, Routledge, Londres, 2018 ; Greenwald G., *No Place to Hide: Edward Snowden, the NSA, and the US Surveillance State*, Macmillan, Londres, 2014.

5 . La trilogie du journaliste James Bamford, bien souvent reprise sans distance par d'autres auteurs va en ce sens. Voir Bamford J., *The Puzzle Palace. Inside the National Security Agency, America's Most Secret Intelligence Organization*, Houghton Mifflin Harcourt, Boston, 1982 ; *Body of Secrets. Anatomy of the Ultra-Secret National Security Agency*, Anchor Books, New York, 2002 et *The Shadow Factory. The Ultra-Secret NSA from 9/11 to the Eavesdropping on America*, Doubleday, New York, 2008.

6 . Pour un exemple de construction d'espace institutionnel, voir notamment Bourdieu P., « Une révolution conservatrice dans l'édition », *Actes de la recherche en sciences sociales,* n°126-127, mars 1999, pages 3-28.

1999 et le printemps 2019 – souvent de manière répétée dans le temps – avec une centaine de professionnels du renseignement par une analyse plus structurale de l'espace des services auxquels ils appartiennent. Pour cela, nous proposerons une analyse de correspondances multiples (ACM), qui permettra, à partir des caractéristiques des services (en termes de missions, d'autorité de référence, de territoire d'action, de volume de personnel, de capital technologique, etc.), de dessiner un espace de positions construit rigoureusement. La mise en relation entre ces positions et les discours des acteurs sur leurs pratiques et le sens du renseignement permet de comprendre les homologies ou, au contraire, les différences irréductibles qui structurent ensuite les coopérations et les types d'échange de données.

Il semble clair, en effet, que ce n'est pas le nombre de traces laissées sur internet qui importe. Ce qui compte, c'est leur constitution en données à des fins de politique de renseignement, c'est l'horizon de suspicion dans lequel elles sont utilisées. Pourquoi intercepter les données ? Parce qu'elles sont simplement disponibles et peuvent être « cueillies » ? Faut-il le faire pour toutes les données de manière à avoir un graphe exhaustif des relations entre des personnes et de larges groupes de populations ou faut-il se restreindre et les laisser où elles sont, en évitant des recoupements non pertinents ?

L'idée d'une surveillance à grande échelle a été banalisée avec l'hypothèse que le branchement des techniques de renseignement sur les technologies automatisées de relevé des traces des activités des individus ou de leurs transactions était légitime, car elle était la contrepartie d'une fonction de protection et de prévention permettant d'anticiper et d'éviter la violence. Seulement ces relations entre l'existence du numérique et un renseignement visant au prédictif n'ont rien d'inéluctables. Elles ont été façonnées politiquement en fonction d'un contexte international et n'ont pas de naturalité technique. Elles dépendent des rapports de force entre les acteurs qui déterminent la valeur d'usage et la valeur d'échange de ces données. Celles-ci sont valorisées en fonction de ce qu'elles peuvent apporter à une orientation de suspicion, tournée le plus souvent sur des actes futurs, mais qui s'estime légitime, y compris quand les corrélations sont si faibles qu'elles ne se transforment pas en évidences judiciaires. C'est là sans doute que cet espace du doute, de la suspicion, des possibles qu'il faut éviter, se distingue des pratiques judiciaires et remplit ce rôle de conseiller du prince avant la décision. Les données de renseignement ont donc aussi une valeur symbolique qui dépend moins de leur contenu – malgré l'idéologie du secret qui sacralise ce contenu –, que de *qui* les a produites, dans quel contexte et pourquoi.

C'est ce dernier point que nous allons détailler car, paradoxalement, il a été masqué par des propos généraux sur la « société de surveillance » et sur le raisonnement algorithmique, quand ce n'est pas sur la servitude volontaire dans laquelle de nombreux internautes du monde entier s'engageraient [7]. Ceci

suppose un retour réflexif pour comprendre ce que les termes de « service de renseignement » ou « services de sécurité » recoupent en réalité et quels rapports leurs pratiques entretiennent avec les modalités de la surveillance passant par des données numériques. Loin d'une certaine tendance des relations internationales à produire des analyses désincarnées, une histoire sans acteurs où les services ne font qu'obéir aux ordres des dirigeants politiques qui détermineraient les stratégies, il est important de signaler les caractéristiques hétérogènes en termes de socialisation, de sens du métier, de missions que les différents services peuvent avoir et les arcs de tension qui existent entre organisations avec des logiques d'action et des modes de raisonnement, sinon antagonistes, du moins fortement décalés et poussant à des stratégies opposées.

Les données comme performances et produits des compétitions entre services de renseignements

Qu'appelle-t-on données lorsque cette terminologie est utilisée à des fins de renseignement politique ? Comment les données sont-elles générées et intégrées à une chaine d'information permettant une analyse répondant aux demandes des hommes politiques ? Quelle place tiennent-elles dans ce que des spécialistes ont nommé un « cycle du renseignement [8] » ? Les données sont-elles – comme ils voudraient le croire – toutes les traces des activités d'une personne et/ou d'un groupe qui ont pu être collectées automatiquement ou intentionnellement et qui sont regroupées dans des dossiers ? Ces données, dites brutes (*raw*), sont-elles des informations génériques en termes de localisation d'une personne associée à un événement, à un moment donné, dans le passé ou au présent, informations qui permettraient dans un deuxième temps, à travers des logiciels algorithmiques d'anticiper des comportements futurs ? Au sein de ces données, peut-on distinguer celles portant sur des contenus et celles dites de connexion ? Quelle est la différence entre celles qui révèlent les opinions personnelles et les « méta-data » qui n'obligent pas à examiner le contenu en tant que tel, mais qui permettent de prouver que des personnes se connaissent et échangent des messages ou partagent des sites particuliers, qu'elles s'intéressent aux mêmes sujets ou qu'elles fréquentent les mêmes lieux, les mêmes amis ? Cette distinction a été présentée par de nombreux services comme pertinente sur le plan technique, et elle supposerait, pour les dernières, une exploitation avec des contraintes plus légères par rapport aux premières [9]. Cette dichotomie continue de se déployer dans différents rapports et

7 . Notamment Lehr P., *Counter-Terrorism Technologies, A Critical Assessment*, Springer, Cham, 2019.

8 . McElreath D., Graves M. et C.J. Jensen III, *Introduction to intelligence studies*, Routledge, Londres, 2017 ; Gill P., Phythian M., « What is intelligence studies? », *The International Journal of Intelligence, Security, and Public Affairs*, vol. 18, n° 1, 2016, pp.5-19 ; Murphy Ch., *Competitive Intelligence: Gathering, Analysing and Putting it to Work*, Routledge, Londres, 2016.

9 . Symboliquement, la tentative de créer une distinction entre les méta-données et les données est un moyen de justifier que les données ne sont pas la propriété de l'internaute. Elle justifie

analyses, en particulier aux États-Unis, mais cette interprétation sur des données techniques impersonnelles est contredite par différentes Cours de l'espace européen, qui ont signalé que l'ensemble des données – qu'elles portent sur le contenu ou soient des données de connexion, de localisation – interfèrent avec la vie privée des personnes et sont donc protégées par les lois et accords internationaux sur les données personnelles [10]. On le voit, la question de la propriété des données est cruciale, de même que celle de la manière dont elles sont constituées et utilisées à différentes fins. Il semble qu'il faille inverser le raisonnement habituel, les données ne sont pas les sources de l'information et de l'analyse, elles en sont le produit.

La propriété des données : une encomienda *électronique*

La question des données et de la définition de ce terme ne peut donc être réglée par un consensus technique. C'est une controverse politique et juridique qui met immédiatement à mal l'idée de données brutes issues d'une propriété technique conservant les traces de la circulation de l'information, mais qui serait indépendante des finalités de son utilisation. Au contraire, il semble que ce soient les différentes finalités qui construisent le sens et la forme des données. Celles-ci ne sont pas naturelles ou brutes, elles sont le produit d'une performance spécifique d'une série d'acteurs.

Ceci n'est pas toujours apprécié à sa juste valeur. Dans les entretiens avec les acteurs des différents services de renseignement ainsi que dans le récit des auteurs se spécialisant sur le « cycle » du renseignement (dans les *intelligence studies* notamment), la question de la nature des données est souvent décrite de manière métaphorique en reprenant des visions physiocratiques ou industrialistes. Ainsi, elles sont parfois présentées comme un aliment ou des fleurs à récolter (semées par les usagers eux-mêmes, au hasard de leurs déplacements, et laissées en friche ou alors échangées contre des services fournis par les entreprises privées et qui dès lors n'appartiennent plus aux individus), et elles se collectent alors comme une manne céleste que l'informatique aurait donnée. Pour les visions plus industrialistes, elles seraient comme un minerai précieux à extraire de sa gangue rocheuse. Il importe d'avoir des outils de forage qui savent détecter ce qui est important et faire des tris qui permettent de ne retenir que ce qui a de la valeur. Au milieu de la masse de données qui circulent et qui sont hétérogènes, faiblement corrélées, il va falloir capter, intercepter et faire remonter celles qui correspondent à un certain profil, afin que, de leur mise en relation, émerge une information, qui doit aussi être affinée, tail-

l'exploitation des données et leur diffusion, leur compilation, leur désagrégation et leur réagrégation en dehors de la connaissance de l'individu qui en est à l'origine.

10. Le 19 octobre 2016, la Cour de justice de l'Union européenne (CJUE) a décidé que l'adresse IP dynamique d'un visiteur du site Web entrait dans les « données à caractère personnel » au titre de la directive 95/46CE (directive sur la protection des données). L'affaire a été introduite par Patrick Breyer, un politicien du Parti pirate allemand.

lée, un peu comme des diamants. Ainsi, l'analyse déboucherait non seulement sur une information de qualité, mais également une information utile dans le processus de décision politique. La production des données transformées en informations par l'analyse des professionnels est alors la qualité même du métier, bien supérieure d'ailleurs aux corrélations statistiques des algorithmes, et à l'idée d'une simple collecte. Mais ces deux métaphores convergent sur l'idée que les données dites brutes n'appartiennent à personne. Pour les deux approches, les individus n'en sont pas propriétaires. Elles sont à la disposition de ceux qui les exploitent et n'ont de valeur que la valeur ajoutée de ceux qui les ont mises en relation et articulées les unes aux autres. Elles ne prennent sens que dans l'information que l'on en tire. Une « *encomienda* » *numérique* est à l'œuvre [11]. Comme lors de la colonisation espagnole, les indigènes (ici les internautes) se sont vus dépourvus de leur droit de propriété et d'un statut de citoyen du web mondial. Ceci a créé les conditions de possibilité d'une « colonisation » du web pour une utilisation à des fins de profit ou de renseignement au nom des bénéfices qu'en tireraient les internautes (consommation mieux ciblée, formation d'amitiés 2.0 sur les réseaux sociaux ou protection contre le terrorisme).

Seulement, cette économie politique primitive à laquelle s'adonnent les services, oublie, volontairement ou non, que les données ont bien une origine, des propriétaires initiaux comme le signalent de manière répétée les cours nationales et européennes, ainsi que les instances de protection des données. La directive GDPR (*General Data Protection Regulation*) de l'Union européenne, qui se veut un exemple pour un nouveau standard mondial, l'a encore réaffirmé [12].

Les données de renseignement : le travail des acteurs et de leurs compétitions

La « fabrique de l'information » et de sa transformation en renseignement, théorisée assez récemment par les *intelligence studies* comme un « cycle » de production afin de justifier une série de pratiques d'interception et de rétention, vise donc à naturaliser l'existence des données pour pouvoir les exploiter et les agréger à des modes de raisonnement souvent déjà construits et qui cherchent davantage une confirmation qu'une invalidation. Mais, à l'inverse, nous soutenons que les données de « renseignement » sont construites performati-

11. L'*encomienda* est un système de travail dans l'empire espagnol où les indigènes étaient censés ne pas avoir de droit de propriété et par lequel la Couronne remettait à une personne privée travaillant pour elle une terre et un certain nombre de natifs qu'elle faisait travailler contre, en théorie, leur évangélisation et leur protection. La relation entre les services, les GAFA et les individus ressemble à cette *encomienda* en refusant aux internautes la propriété de leurs données et le travail qu'ils font pour les produire et même les diffuser.
12. Le General Data Protection Regulation 2016/679 est un règlement du droit de l'Union sur la protection des données et la vie privée pour tous les individus au sein de l'Union européenne et de l'espace économique européen. Il aborde également l'exportation de données à caractère personnel en dehors des zones de l'UE et de l'EEE. Il est entré en vigueur le 25 mai 2018.

vement par les décisions politiques qui initient leur « recherche » proactive et par l'usage social des techniques de surveillance visibilisant ou non certains éléments, ainsi que par les langages qui leur permettent d'être encodées et décodées, par tous, par un destinataire unique ou des destinataires non voulus qui les interceptent. Les performances des acteurs du renseignement se fondent donc sur des données appartenant à des individus, mais très souvent, ils les sérialisent, les anonymisent, les regroupent par dossiers et surtout fabriquent des récits spécifiques qui colonisent les données individuelles pour les organiser en « outils de renseignement [13] ». Ces traces ne deviennent donc des données que dans la mesure où il y a un intérêt politique à les produire et à les conserver, à en établir les frontières et à discriminer ce qui est retenu de ce qui est écarté. Elles s'établissent en vue d'établir des listes de menaces, de risques, de vulnérabilités à partir desquelles on sérialise des suspects.

Notre vision en termes de « *data politics* » insiste dès lors sur le fait que les données sont des performances particulières qui reconfigurent les rapports entre le digital et le matériel, et influent sur les relations contemporaines entre le renseignement, la surveillance, la violence et l'obéissance en fonction des jeux internes des acteurs et de leurs définitions de ce qu'est la sécurité et l'insécurité [14]. Les données de renseignement sont ainsi le produit d'un travail qui, d'entrée de jeu, les constitue pour ce qu'elles sont « données à voir », comme si elles étaient neutres et objectives. Mais en réalité, les mises en relation, les mécanismes d'association, de connexion, de filtre, de profilage, qui concernent des individus en relation dont certains sont plus suspects que d'autres, plus indésirables que d'autres et plus menaçants pour l'ordre établi, restent une opération proprement politique.

Les données de renseignement ne sont donc que rarement les sources permettant d'établir des causalités, elles sont au contraire une prestation, un résultat du processus qui légitime ou non les suspicions aux yeux des acteurs mais qui se fondent uniquement sur des corrélations et non des évidences. D'où les luttes structurelles entre les autorités judiciaires et les services de renseignement. Ce sont les interprétations, les portraits dressés à partir des profils qui créent les conditions du spectacle, de la dramaturgie que les services mettent en œuvre avec leurs listes de suspects et leurs analyses opérationnelles des futurs possibles. Ces interprétations sont la base même des dossiers sur lesquels les différents services travaillent.

Seulement ces dossiers qui auparavant étaient matériellement écrits sur papier sont maintenant pour la plupart inscrits sur un support informatique.

13. Bigo D,. « Sécurité maximale et prévention ? La matrice du futur antérieur et ses grilles », in Cassin B. (dir.), *Derrière les grilles : sortir du tout évaluation*, Fayard, Paris, 2013.
14. Bigo D., « Globalized (In)Security: The field and the Ban-Opticon », in Bigo D., Tsoukala A. (dir.), *Terror, Insecurity and Liberty. Illiberal practices of liberal regimes after 9/11*, Routledge, Londres, 2008.

Est-ce que cela les affecte et change le mode de raisonnement ? Certains auteurs, suivant le *materialist turn* proposé par les approches STS (sciences-technologie-société), comme Marieke de Goede le pensent et voient là des transformations profondes. Mais rien n'est moins sûr [15]. Celles-ci semblent toucher les franges du métier, les services qui s'occupent de la mobilité des voyageurs, ou des opérations financières suspectes, mais peu les services secrets eux-mêmes. L'idée d'une gouvernance par les données que développe Mathias Leese, a ainsi une certaine validité mais les exemples précis viennent des pratiques de contrôle aux frontières liées à l'interopérabilité des bases de données, aux « scores de suspicion » et aux analogies qui sont faites avec le contrôle des flux financiers, pour qui cette gouvernance semble centrale [16]. En revanche pour la plupart des services de renseignement, intérieurs comme extérieurs, le raisonnement indiciel dont parle Carlo Ginzburg reste au cœur des pratiques de nombreux agents qui aiment le « *low tech* », et il n'est pas certain qu'on puisse lui opposer un mode de raisonnement « algorithmique » qui se substituerait au premier et serait fondé sur des corrélations à grande échelle, sur des « possibilités » plutôt que sur des chaines de causalités précises, avec un mode de raisonnement spéculatif propre à l'outil informatique [17]. Dans nos terrains récents, la réflexion continue de s'organiser partout autour de dossiers, d'archives qui ne sont partagées que par un petit groupe de professionnels, qui les lisent en fonction de certaines autres informations jugées secrètes et opérationnelles. La valeur des informations tirées des données est donc loin d'être égale. Si certaines sont utiles à l'identification bloquant l'anonymat quasi structurel de l'internet, si d'autres servent à la localisation, pour de nombreux acteurs, l'accumulation de données hétérogènes peut contrevenir à la compréhension des actions. Le raisonnement par corrélation des algorithmes manque ses cibles individuelles, il crée des culpabilités par association. C'est pourquoi le mode de raisonnement indiciel basé sur le soupçon va éventuellement intégrer la spéculation et les possibilités, mais il restera le cœur du métier

15. On pourrait dire que de nombreux débats sur les échanges de données en matière de renseignement se basent sur les potentialités offertes par la technologie plus que sur les pratiques effectives des services. Or, il en va de la régulation de la technique comme de la régulation routière. Ce n'est pas parce qu'un véhicule peut rouler à 200 kilomètres heure en permanence qu'il est autorisé à le faire et que le conducteur le fait. Le juridique est là pour poser des limites aux potentialités techniques… Des auteures comme Louise Amoore et Marieke de Goede ont parfois posé en termes équivalents les pratiques et les potentialités, ainsi que les conditions du présent et les tendances émergentes. Cela a amené à une vue par trop programmatique des intentions des services, en particulier des nouveaux venus comme s'ils étaient emblématiques de changements paradigmatiques là où il y a des luttes que ces prétendants peuvent très bien perdre, en particulier sur la validité de l'accumulation et de la rétention des données, et sur la précision des algorithmes prédictifs. Voir notamment De Goede M., *Speculative Security: The Politics of Pursuing Terrorist Monies*, University of Minnesota Press, Minneapolis, 2012 et Amoore L., Raley R., « Securing with Algorithms: Knowledge, Decision, Sovereignty », *Security Dialogue*, vol. 48, n° 1, 2017, pp. 3-10.
16. Leese M., « The New Profiling: Algorithms, Black Boxes, and the Failure of Anti-Discriminatory Safeguards in the European Union », *Security Dialogue*, vol. 45, n° 5, 2014, pp. 494-511.
17. Bonelli L., Ragazzi F., « Low-tech security: Files, notes, and memos as technologies of anticipation », *Security Dialogue*, vol. 45, n° 5, 2014, pp. 476-493.

qui suppose *in fine* des individus à étudier, à discipliner et éventuellement à châtier. Sans cela le métier ne serait plus qu'une géopolitique généralisant des tendances, projetant des futurs, mais sans opérationnalité. Les professionnels des services insistent sur ce dernier point pour se distinguer des cabinets de consultants (privés) travaillant sur des *open sources*, qui, au contraire, valorisent tapageusement les *big data analytics* et leurs prévisions, souvent parce qu'ils n'ont rien d'autre à vendre.

Une large partie des études de surveillance, bien que critiques sur de nombreux domaines, font de la production et de la traçabilité des données, le produit inévitable de la société moderne, qui la rendrait « plate », « rhyzomatique », à partir des « *exhaust data* » se diffusant entre tous les mondes sociaux et internationaux. Si effectivement la traçabilité s'automatise et permet l'accumulation rapide, signalons que certains auteurs généralisent trop vite et n'insistent pas assez sur cet élément de constitution des données qui les particularise, fragmente leur signification et les intègre comme un produit politique. Ces études confondent dès lors les politiques des mondes du renseignement, leur verticalité, leurs compétitions, et les procédés techniques de surveillance que ces derniers utilisent.

Si certains de ces procédés de surveillance sont transversaux et horizontalisent les techniques en facilitant les transmissions d'information à distance, cela ne veut pas dire qu'il en découle une homogénéisation des logiques d'action et des ressorts de ce que recherchent concrètement les agents. Trop de théories de la surveillance électronique ne distinguent pas assez les mondes sociaux et pensent que les effets du monde digital sont uniformes et liés à la seule technologie. La production de données numériques dans l'univers de la santé, du commerce, ou du renseignement ne débouche en aucun cas sur les mêmes effets. Les acteurs usent des nouvelles technologies en fonction de leurs dispositions passées, de la facilité ou non de la re-constitution des données papiers en données informatiques tant sur le plan technique qu'en termes de secret, de confidentialité et d'intérêt ou non à les conserver et/ou à les diffuser. Les données du monde numérique affectent les formes de pouvoir et les formes politiques du quotidien mais l'inverse est bien sûr vrai. Elles sont simultanément intégrées dans les univers sociaux, dans les pratiques ordinaires uniquement si elles peuvent se modeler et s'articuler aux anciens usages en fonction des enjeux de pouvoir des acteurs et les aider dans leurs luttes.

La technologie informatique ne « révolutionne » donc pas tant le renseignement qu'elle se moule sur les usages sociaux différentiés qu'elle amène dans les pratiques routinières des différents mondes de ce renseignement politique. Elle en renforce les clivages, les arcs de tension existants. Il convient donc de rester particulièrement prudent face aux discours triomphants qui décrivent le renseignement comme surveillance à grande échelle mais à dis-

tance, analysant des tendances pour accéder à une dimension préventive et prédictive *via* les opérations de « *data derivative* [18] ». Cette vision favorise les acteurs qui la produisent, en relativisant l'apport des agents et opérations de terrain, valorisant à l'inverse l'accumulation de données hétérogènes qui peuvent malgré tout, grâce à l'analytique algorithmique des *Big data* sur les signaux faibles, mettre en lumière des corrélations que l'esprit humain n'aurait pas faites. Elle n'est qu'un des récits dont se servent les agents les plus intéressés aux définitions du renseignement comme anticipation d'actes hostiles d'où qu'ils proviennent ; une conception qui convient sans doute bien aux nouveaux entrants dans cet espace, et qui ne peuvent agir qu'à distance car ils n'ont pas vraiment d'agents de terrain et doivent trouver des « relais ». Sans surprise, elle est en revanche loin de convaincre les acteurs les plus anciens, qui ont des capacités opérationnelles, qui pensent en termes d'adversité ou inimitié et éventuellement en termes de suspects mais qui se méfient profondément de la désindividualisation, des théologies sur la possibilité de connaitre l'inconnaissable, et de planifier le futur comme s'il était un futur antérieur. Les luttes symboliques sur la valeur du renseignement et sur ces procédés sont alors engagées et déterminent le sens de ce que sont les « données ».

Les trois espaces que nous allons étudier maintenant sont tous soumis à une reformulation de leurs pratiques par l'intégration des enjeux sociotechniques du digital, mais chacun garde profondément la capacité à cadrer et structurer ce que l'on appelle des données de renseignement et les outils que l'on utilise. À ceux qui seraient tentés de penser des mutations technologiques comme une révolution des pratiques, on peut rappeler le poids des routines professionnelles et des catégories institutionnelles de perception du monde social dans les pratiques sociales. Les évolutions qu'impliquent les transformations techniques et les opportunités nouvelles qu'elles offrent viennent en effet s'articuler avec du déjà-là, en termes de socialisations professionnelles et de routines de travail. Les changements qui peuvent advenir sont dès lors graduels et s'intègrent dans des missions, des savoirs et des finalités existant de longue date. L'analyse doit donc suivre l'étroite ligne de crête entre « l'illusion du jamais vu et l'illusion du toujours ainsi », pour reprendre la jolie formule du politiste Bernard Lacroix [19].

18. Le *data derivative* est issu d'un amalgame de données ventilées reagrégées par le biais de règles d'association mobiles basées sur des algorithmes et visualisées en « temps réel » comme carte de risque, score ou drapeau à code couleur.
19. Lacroix B., « Retour sur 1848 : Le suffrage universel entre l'illusion du "jamais vu" et l'illusion du "toujours ainsi"», *Actes de la recherche en sciences sociales*, n° 140, 2001, pp.41-50.

L'espace transnational du renseignement : positions, dispositions et pratiques professionnelles

Les études sur le renseignement souffrent souvent d'une forme de nationalisme méthodologique qui présuppose une communauté de renseignement fondée sur la défense d'un intérêt et la mise en œuvre d'une stratégie de sécurité proprement nationaux. Les interceptions de données sont lues différemment selon qu'elles concernent les citoyens et les non-citoyens et les échanges considérés comme hors des pratiques routinières dès qu'il s'agit de services étrangers. Nombre d'ouvrages laissent aussi penser que les différents services sont réticents à ces échanges de données, qu'ils sont très étroitement encadrés par des accords secrets, et qu'ils reposent sur une confiance mutuelle issue du combat contre des ennemis communs durant la Seconde Guerre mondiale ou durant la guerre froide. Si tout n'est pas erroné dans ce point de vue, il reste trop schématique.

La recherche suggère au contraire que pour le contre-terrorisme « global », et sans doute à la différence d'autres missions, les logiques transnationales sont plus fortes que celles purement nationales. Ceci tient à ce que les données de renseignement sont constituées par les types de questions posées et les modes de raisonnement impliqués. Les communications apparaissent donc plus faciles entre services appartenant à des pays différents mais ayant les mêmes visions et pratiques sur le sujet qu'elles ne le sont entre services du même pays, mais déployant des savoir-faire différents ou même complémentaires.

Il faut donc comprendre les raisons d'émergence de ce que l'on a appelé des réseaux transgouvernementaux entre les agences de renseignement, ou plus précisément des guildes transnationales qui regroupent les agences spécialisées dans les mêmes missions et dont les agents ont des dispositions, des socialisations, voire des *habitus* professionnels homologues, qui leur permettent de surmonter les différences nationales [20]. Les loyautés entre ces agences sont parfois plus fortes que leur attachement institutionnel aux hommes politiques de leur pays comme l'ont montré plusieurs cas récents dont celui du BND (*Bundesnachrichtendienst*) allemand, dont un département a été amené à confier des éléments confidentiels de la politique du gouvernement d'Angela Merkel à ses alliés de la NSA dans le cadre d'échanges routiniers [21].

20. Voir notamment Bigo D., « Pour une sociologie des guildes transnationales », *Cultures & Conflits*, n° 109, 2018, pp. 9-38 et « Beyond national security, the emergence of a digital reason of state(s) led by transnational Guilds of Sensitive Information. The case of the Five Eyes Plus Network », in Wagner B., Kettemann M.C. et K. Vieth (dir.), *Research Handbook on Human Rights and Digital Technology: Global Politics, Law and International Relations*, Elgar Publishing, Londres, 2018.
21. Hegemann H., Kahl M., « (Re)Politisierung der Sicherheit? », *ZIB Zeitschrift für Internationale Beziehungen*, vol. 23, n° 2, 2016, pp. 6-41.

Il existe donc bien un espace transnational du renseignement constitué de différents regroupements de services coopérant ensemble dans la gestion des données numériques et des informations sensibles en général. Cet espace n'est pas divisé en fonction des politiques nationales des gouvernements – même si elles jouent un rôle par les structures de coordination qui existent – mais en fonction des types de renseignement recherchés, des caractéristiques de ces services, de leur composition et de leurs pratiques.

Des relations entre trois univers aux logiques distinctives qui reposent sur des pratiques différentes du métier de renseignement ?

Afin de préciser cette hypothèse de travail, nous avons donc construit une première ébauche d'un espace transnational des agences de renseignement dans les pays qui s'accordent pour se dire des démocraties et ont en même temps des prétentions régionales ou globales de politique étrangère. Pour cela, nous avons eu recours à une analyse de correspondances multiples (ACM), qui permet de distribuer mathématiquement les services, en les rassemblant en fonction de leurs ressemblances et de leurs différences les plus significatives. L'ACM permet d'objectiver certaines caractéristiques saillantes de la population étudiée, d'opérer des regroupements qui ne doivent rien au hasard et de les visualiser sous forme de graphiques, dont les axes résument les corrélations entre les variables. Elle permet ainsi de systématiser les données plus qualitatives recueillies lors d'entretiens [22].

La taille des services américains, comme leurs budgets explique qu'ils aient été à l'initiative et sont souvent à la tête de ces réseaux entre alliés qui tissent ce soi-disant Nord global et qui se projettent aussi hors de l'espace des démocraties libérales [23]. Le plus connu de ces réseaux est celui des *Five Eyes* qui relie les agences traitant des données liées aux communications satellitaires, électroniques et internet (États-Unis, Grande Bretagne, Canada, Australie et Nouvelle Zélande). Son activité avait d'abord été mise en lumière en 1988 par le journaliste Duncan Campbell, au sujet du projet Echelon, un système automatisé d'écoute des communications transitant notamment par les satellites de télécommunications internationaux [24]. Mais ce sont les divulgations d'Edward Snowden sur les activités de la NSA qui lui ont valu la célé-

22. Sur son usage dans l'enquête, voir notamment Renisio Y., Sinthon R., « L'analyse des correspondances multiples au service de l'enquête de terrain. Pour en finir avec le dualisme "quantitatif"/"qualitatif" », *Genèses*, n° 97, 2014, pp. 109-125. Voir aussi Le Roux B., Rouanet H., *Multiple correspondence analysis*, Thousand Oaks, Sage Publications, 2010.
23. Bigo D., Bonelli L. et T. Deltombe (dir.), *Au nom du 11 septembre. Les démocraties à l'épreuve de l'anti-terrorisme*, La Découverte, Paris 2008.
24. Campbell D., « Somebody's listening », *New Statesman*, 18 août 1988. Voir également Commission temporaire sur le système d'interception ECHELON, *Rapport du Parlement européen sur l'existence d'un système d'interception mondial des communications privées et économiques (système d'interception ECHELON)*, Bruxelles, 2001/2098(INI).

brité qui est la sienne aujourd'hui. Ce réseau s'est étendu bien au-delà de son nom, et il n'est pas rare de voir signaler que les *Five Eyes Plus* sont neuf (*Nine Eyes*), incluant les services ou les départements internes de certains services que la France, l'Allemagne, l'Espagne ou la Suède ont mis en place pour l'interception des données passant par les câbles sous-marins et terrestres numériques [25]. Sur cette base, nous avons retenu une liste de 25 services appartenant à ces 9 pays. Il s'agit des principaux services (policiers ou non) de lutte antiterroriste et de contre-espionnage, des services de renseignement extérieurs et, s'ils existent les services techniques dédiés aux interceptions de données à grande échelle. L'activité des services de renseignement militaires concernant surtout des enjeux propres à l'armée, ils ont été provisoirement écartés, même s'ils peuvent parfois jouer un rôle en matière de diplomatie, de lutte anti-terroriste et s'ils interviennent parfois sur leur propre territoire [26]. Il en va de même des services de renseignement financiers, parfois mobilisés dans la lutte contre le terrorisme, mais dont l'essentiel de l'activité porte sur l'anti blanchiment [27], ainsi que des agences de contrôle des frontières.

Bien que les effectifs demeurent ici faibles, cette ACM permet de construire ces deux graphes : le premier sur les modalités les plus significatives de cet espace transnational qui recensent les différents types de capitaux que les différents services possèdent ainsi que leurs attributs organisationnels et leurs objectifs, le second identifiant à partir de ces propriétés objectives, les proximités et les distances entre les services et permettant de visualiser des sous-groupes ou univers spécifiques partagés par des acteurs.

25. Certains journalistes ont même parlé des *14-eyes* avec la Belgique, les Pays-Bas, l'Italie, la Norvège et le Danemark.
26. Voir notamment Rios Bordes A., *Les savoirs de l'ombre. La surveillance des populations aux États-Unis (1900-1941)*, Paris, EHESS éditions, 2018, ainsi que son article dans ce numéro.
27. Voir la contribution d'Anthony Amicelle dans ce numéro.

Encadré méthodologique

Pour les États-Unis, nous avons sélectionné les services suivants : National Security Agency (NSA), Central Intelligence Agency (CIA) et Federal Bureau of Investigation (FBI) [28] ; pour le Canada : Canadian Security Intelligence Service (CSIS) et Communications Security Establishment (CSE) ; Pour le Royaume Uni : Counter Terrorism Command (CTC), Security Service (MI5), Secret Intelligence Service (SIS ou MI6) et Government Communications Headquarters (GCHQ) ; pour La Nouvelle Zélande : New Zealand Security Intelligence Service (NZSIS) et Government Communications Security Bureau (GCSB) ; pour l'Australie : Australian Signals Directorate (ASD), Australian Security Intelligence Organisation (ASIO), Australian Secret Intelligence Service (ASIS) ; pour la France : Direction générale de la Sécurité extérieure (DGSE), Direction générale de la Sécurité intérieure (DGSI) et Service central du renseignement territorial (SCRT) ; pour l'Allemagne : Bundesnachrichtendienst (BND), Bundesamt für Verfassungsschutz (BfV) et Bundeskriminalamt (BKA) ; pour l'Espagne : Centro Nacional de Inteligencia (CNI), Comisaría General de Información (CGI) et Servicio de Información de la Guardia Civil (SIGC) ; et pour la Suède : Försvarets Radioanstalt (FRA) et Säkerhetspolisen (Säpo).

Pour ces vingt-cinq services, nous avons conservé neuf variables actives pour l'analyse :

1. Le territoire de compétence, avec trois modalités : interne, externe, et interne/externe.

2. L'habilitation judiciaire des agents, avec deux modalités : oui et non.

3. Les capacités opérationnelles, c'est-à-dire l'existence d'agents de terrain, avec deux modalités : oui et non.

4. Les objectifs assignés aux services, avec deux modalités : la lutte contre les menaces intérieures ou la défense de l'intérêt national (qui inclut l'espionnage).

5. Le nombre de personnel, avec trois modalités : de 0 à 1 999, de 2 000 à 4 999 et plus de 5 000.

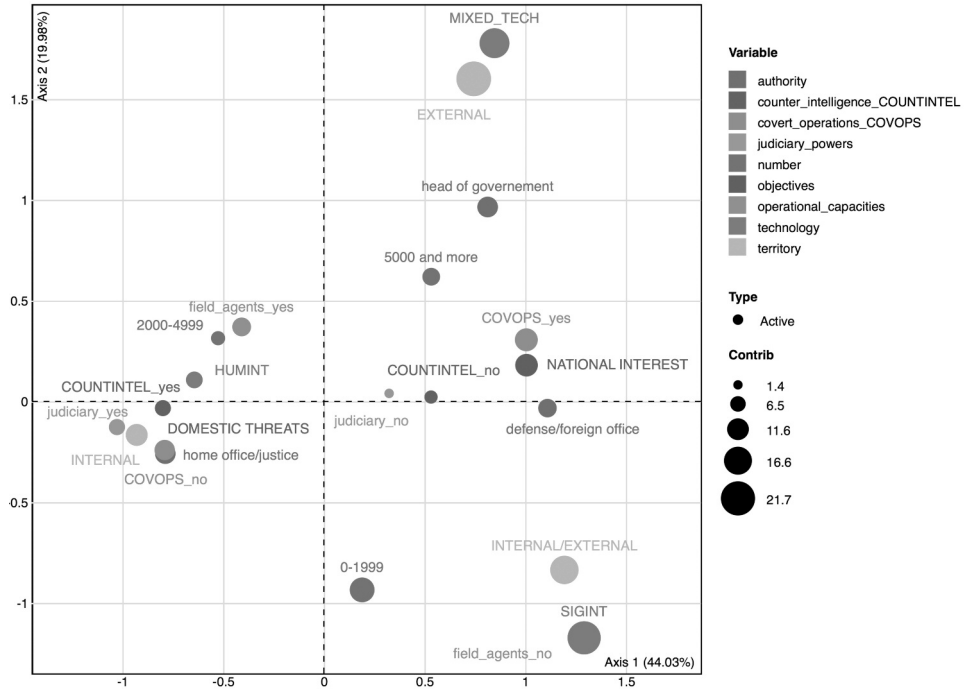
6. Les technologies utilisées, avec trois modalités : le renseignement humain (HUMINT), le renseignement technologique (SIGINT) et des capacités mixtes (MIXED_TECH).

7. L'autorité de rattachement, avec trois modalités : ministère de l'Intérieur ou de la Justice, ministère de la Défense ou des Affaires étrangères, et chef du gouvernement.

8. Existence d'une activité de contre-espionnage, avec deux modalités : oui et non

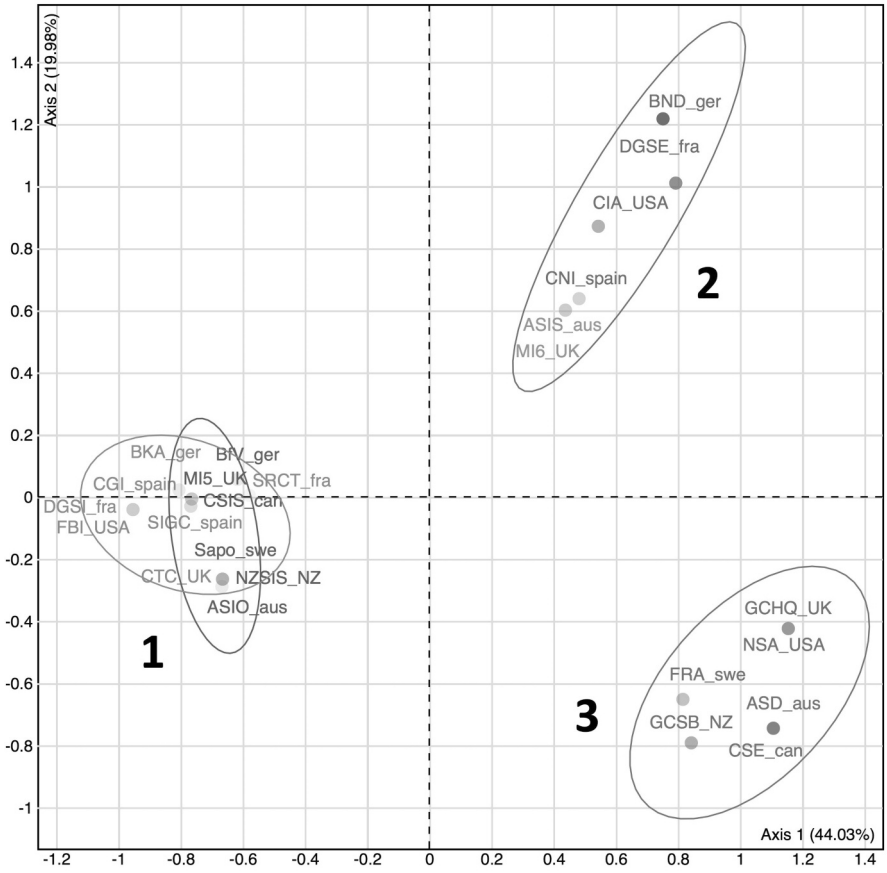
9. la capacité à mener des opérations clandestines (*covert operations*), avec deux modalités : oui et non.

28. Compte tenu de la variété des missions du FBI, à la fois police criminelle et service de renseignement intérieur, on a ici seulement pris en compte les 3 600 agents de la *Counterterrorism Division*.



Graphique 1. Modalités les plus contributives sur les axes 1 et 2 de l'ACM

Les axes 1 et 2 de l'ACM résument à eux seuls plus de 64% des données (respectivement 44,03% pour l'axe 1 et 19,98% pour l'axe 2). Sur l'axe 1, les modalités les plus contributives opposent, à gauche (valeurs négatives), les menaces domestiques (7,8%), l'interne (7,8%), l'absence d'opérations clandestines (6,1%), l'activité de contre-espionnage (4,5%), le rattachement aux ministères de l'Intérieur et de la Justice (6,1%), les pouvoirs judiciaires (4,4%) et le renseignement humain (4,6%), et à droite (valeurs positives), l'intérêt national (8,5%), l'interne/externe (7%), les opérations clandestines (7,8%), le rattachement aux ministères de la Défense ou des Affaires étrangères (6%), et le renseignement technologique (7%) ou mixte (1,5%). Sur l'axe 2, les modalités les plus contributives opposent en bas (valeurs négatives), le renseignement technologique (12,7%), l'absence d'agents de terrain (12,7%) et l'interne/externe (7,5%) et en haut (valeurs positives) le renseignement mixte (14,6%), la présence d'agents de terrain (4%) et l'extérieur (19,7%). Ces distributions des propriétés de chacun des services étudiés permettent ensuite d'observer leur distribution dans l'espace en trois ensembles distincts (graphique 2).



Graphique 2. L'espace des positions institutionnelles

Le premier pôle (1) sur la gauche, en milieu de tableau découpe un espace de proximité entre les services qui sont en priorité de recrutement policier et s'occupent d'abord des enjeux internes. Ceux-ci sont avant tout concernés par les menaces intérieures, même s'ils développent des capacités d'action et des coopérations, de sorte à pouvoir prévenir celles émanant d'acteurs provenant de l'étranger. Leurs missions relèvent principalement de deux grands domaines : la subversion politique (qui inclut l'antiterrorisme, mais ne s'y limite pas) et le contre-espionnage. Ils dépendent des ministères de l'intérieur ou de la justice.

En leur sein, on peut distinguer deux sous-ensembles : ceux qui sont dotés, au moins partiellement, de pouvoirs judiciaires et qui sont des *Law enforcement agencies*, de ceux qui n'en possèdent pas. Parmi les premiers, on compte le BKA allemand, la CGI et le SIGC espagnols, le FBI états-unien et la DGSI française. Parmi les seconds, le BfV allemand, le MI5 et le CTC bri-

tannique, le Säpo suédois, le CSIS canadien, l'ASIO australien, le NZSIS néozélandais et le SCRT français. Au sein de ce pôle, l'évolution des nouvelles technologies de l'information et de la communication (NTIC) est présentée dans les entretiens à la fois comme une contrainte et comme une ressource.

Une contrainte, d'abord, en raison des flux d'informations qui sont désormais générés par les individus. L'élément de base du travail des services de renseignement intérieurs est en effet la fiche, portant sur un individu ou une organisation. Avant même que la mécanographie, puis l'informatique n'étendent son importance, cette fiche sert à consigner toutes les informations recueillies. La rencontre avec une source ouverte – politique, syndicale, associative, religieuse ou autre – est le plus souvent reportée par écrit, et celle avec un « indicateur » se prolonge par la rédaction d'une note de contact relativement complète, à laquelle le fonctionnaire adjoint ses commentaires et son analyse. Il en va de même pour les informations transmises par d'autres services nationaux ou étrangers ou pour celles collectées en utilisant les techniques dites de « milieu fermé » : filatures, écoutes téléphoniques, « sonorisation » de lieux privés (pose de microphones) ou visites domiciliaires discrètes. Plusieurs notes peuvent ensuite être mobilisées pour établir, avec d'autres éléments (documentation interne d'une organisation, articles de presse généraliste ou militante, comptes rendus d'écoutes téléphoniques ou de surveillance, etc.), des biographies d'individus ou d'organisations, dont le rôle apparaît significatif dans un secteur déterminé, puis pour les actualiser. Si nécessaire, celles-ci peuvent être transformées en dossiers judiciaires, c'est-à-dire recevables lors d'un procès.

Or, comme l'expliquent les agents, les cibles de la surveillance produisent désormais des quantités de données plus considérables que par le passé. Ainsi, entre février 2014 et novembre 2014, un individu parti ensuite en Syrie a échangé pas moins de 33 438 SMS et 2 802 appels téléphoniques avec 300 correspondants. Son compagnon de voyage en comptabilisait pour sa part respectivement 35 107 et 1 606 entre mai et septembre 2014. Dans des dossiers qui impliquent plusieurs dizaines d'individus, on perçoit immédiatement le volume de données à traiter, auquel s'ajoutent bien entendu celles qui proviennent des réseaux sociaux de type Facebook et des messageries comme Skype, WhatsApp, Telegram ou Messenger. On mesure la distance par rapport à l'époque, pas si lointaine, où les communications filaires se comptaient en dizaines sur des affaires de ce type. Ce volume interdit en effet une analyse qualitative *a priori* de l'ensemble de ces données.

Pour autant, la quantité de traces numériques laissées par les individus constitue également une ressource appréciable pour les agents du renseignement. Outre les communications téléphoniques, les SMS attestent par exemple de la fréquence des contacts entre des individus qui jusqu'alors auraient eu

recours à des canaux de communication autres et qui n'auraient peut-être pas été remarqués. Savoir que les deux individus mentionnés dans l'affaire évoquée ci-dessus ont échangé 40 communications dans les 24 heures précédant leur départ constitue une information de valeur.

De plus, la communication numérique permet de localiser les individus. La géolocalisation des téléphones portables permet par exemple d'attester de la co-présence de deux personnes au même endroit. Dans une autre affaire de départ en Syrie, un policier remarque dans un procès-verbal que les « deux protagonistes ont déclenché des relais similaires sur des journées et créneaux horaires identiques », alors même qu'il n'y avait apparemment aucun lien téléphonique entre eux. Ce qui lui permet de conclure : « vu ces éléments, il est fortement plausible de penser que ces deux protagonistes se connaissaient et s'étaient déjà rencontrés physiquement bien avant de se joindre directement l'un et l'autre à partir de leurs lignes respectives ». De la même manière, la consultation et l'actualisation d'un site Facebook permet également de situer un internaute. Ainsi, le trajet d'un jeune Français parti combattre en Irak peut-il être retracé à partir de ses adresses IP de connexion. Le 2 janvier 2015, il était à son domicile en région parisienne, les 4 et 5 janvier, il se connecte depuis la Turquie et à partir du 8, de l'Irak.

Enfin, le simple historique des communications permet également de savoir quels sites internet ont été consultés. Les dossiers regorgent ainsi d'informations sur les requêtes concernant par exemple des billets d'avion ou la consultation de sites djihadistes.

Ces informations ne disent rien du contenu des communications, mais elles dessinent des réseaux de relations, attestent de leur densité et de leur étendue, et le cas échéant de leur situation géographique. Il suffit de voir l'un des graphes qu'elles permettent d'établir pour se rendre compte de leur utilité dans la compréhension de la vie d'un individu. On peut d'ailleurs inviter le lecteur qui possèderait un compte Gmail ou Yahoo à en faire une expérience pratique à partir du programme Immersion, développé par le Massachusetts Institute of Technology (MIT) [29].

À un stade plus avancé des enquêtes, lorsque les agents du renseignement peuvent avoir accès physiquement aux ordinateurs et aux téléphones portables, ils bénéficient d'une mine supplémentaire d'informations, qui les renseignent cette fois sur le contenu de ces échanges. Les SMS, les conversations sur les réseaux sociaux, les documents téléchargés (textes, images, vidéos) et même les recherches internet leur deviennent accessibles. L'exploitation du téléphone portable d'un jeune Français mis en examen pour tentative d'attentat révèle ainsi qu'il se documentait régulièrement, *via* Telegram, sur la manière

29. https://immersion.media.mit.edu/ Consulté le 30 septembre 2019.

de le commettre. Il téléchargeait des documents expliquant la fabrication d'explosifs, consultait régulièrement des vidéos d'exécutions commises par l'État islamique ainsi que du contenu de propagande telles que des vidéos faisant l'apologie des attentats de *Charlie Hebdo* ou de l'attaque du Bataclan. Les policiers trouvaient également un historique de ses échanges avec deux djihadistes combattant dans la zone irako-syrienne. Ses recherches sur Google faisaient quant à elles apparaître « boite gay », « adresse personnelle policier », « adresse Marc Trévidic » (un ancien juge d'instruction anti-terroriste médiatique), laissant penser qu'il souhaitait s'en prendre à la communauté LGBT, à des policiers ou des juges.

Si personne ne se plaint de ces masses de données disponibles, la question de leur exploitation est souvent pointée comme l'un des points faibles des services de renseignement. « Nous ne manquons pas de données ni de métadonnées, mais nous manquons de systèmes pour les analyser » expliquait ainsi Patrick Calvar, alors directeur de la DGSI aux parlementaires [30].

L'une des pistes évoquées est l'utilisation de logiciels informatiques. Certains permettent ainsi de dessiner des graphes de relations, à partir de corrélations, par exemple entre les numéros appelés, entre des localisations dans des créneaux de temps déterminés, mais aussi avec de nombreux autres éléments issus des enquêtes (auditions de témoins, interrogatoires, perquisitions, etc.). En France, la police judiciaire et la gendarmerie les utilisent depuis quelques années pour des affaires complexes. Le plus célèbre est Analyst's Notebook, développé à l'origine par une société canadienne, rachetée par IBM [31]. Mais dans le renseignement, les méthodes semblent restées plus longtemps artisanales. Si la *Comisaría General de Información* espagnole utilise Analyst's Notebook, ce n'est qu'en 2017 que la DGSI a passé un contrat controversé avec l'entreprise américaine Palantir, afin de se doter d'un outil similaire et le SCRT n'en bénéficie toujours pas.

Une seconde difficulté concerne les contraintes pratiques de cette collecte de données, dont on aurait tort de penser qu'elle se fait toute seule. Il faut non seulement obtenir parfois des autorisations judiciaires, mais également solliciter l'ensemble des opérateurs concernés. Lorsqu'un individu suspect est identifié, qu'un juge a autorisé que l'on recueille ses données téléphoniques ou de connexion, il faut ensuite contacter tous les opérateurs de téléphonie, afin de savoir s'ils ont une ligne à son nom, puis demander les factures détaillées. Il en va de même pour une demande de géolocalisation. Ceci implique un travail considérable de la part des enquêteurs, mais également un coût important pour les services. Les compagnies de téléphone facturent en effet leurs services. Ainsi, dans l'un des dossiers étudiés, les policiers sont conduits à renon-

30. Audition devant la Commission de la défense nationale et des forces armées, 10 mai 2016.
31. https://www.ibm.com/fr-fr/marketplace/analysts-notebook Consulté le 30 septembre 2019.

cer à leur requête en raison du montant « devenu astronomique » de leur demande, évaluée à plus de 9 200 euros hors taxes, pour un seul numéro sur quelques jours. Les tarifs des prestations des opérateurs ont fait l'objet d'une négociation avec l'État. En France, en 2010, l'identification d'un abonné mobile à partir de son numéro d'appel coutait 6,50 euros, la géolocalisation du trafic 35 euros par mois hors taxe, auxquels s'ajoutaient 0,08 euros hors taxes par « hit » envoyé durant la période. Le coût des interceptions judiciaires (écoutes téléphoniques, factures détaillées, données de géolocalisation) atteignait ainsi 122,55 millions d'euros en 2015 (contre 89,78 en 2005), dont 61,4 étaient payés aux prestataires privés [32]. L'Espagne a résolu ce problème en intégrant l'ensemble des opérateurs de téléphonie dans SITEL (*Sistema Integrado de Interceptación de Telecomunicaciones*), qui permet aux services d'accéder directement aux numéros qui les intéressent. Une voie similaire a été développée en France avec la mise en place d'une plateforme nationale des interceptions judiciaires (PNIJ) permettant les écoutes, les réquisitions de facture détaillées, l'identification des numéros, la géolocalisation en temps réel et l'interception des flux internet. Initialement prévue pour 2008, elle a connu une série de difficultés techniques qui l'ont empêchée d'être pleinement opérationnelle. Une nouvelle version est prévue pour 2024. Néanmoins, si l'on en croit le ministère de la Justice, en 2017, elle avait permis 8 500 interceptions judiciaires, 2 millions de demandes d'obtention de données par an, et comptabilisait 45 000 utilisateurs réguliers, 7 000 connexions par jour, 600 000 communications et 900 000 SMS interceptés chaque semaine [33].

Ces dimensions pratiques de la collecte de données et de leur analyse expliquent les pressions des services de renseignement pour obtenir des modifications législatives. La première concerne les durées de conservation des données, de la part des opérateurs. L'impossibilité de traiter ces volumes considérables en temps réel s'accompagne d'une pétition de conservation plus longue. Plusieurs agents interrogés expliquent qu'ils veulent pouvoir accéder à l'historique d'un individu, même des années plus tard, s'il apparaît dans une enquête. Revenir rétrospectivement sur ses contacts et sa localisation leur permet en effet de nourrir le travail présent. Une pétition qui s'oppose toutefois à plusieurs décisions de la Cour de justice des Communautés européennes (CJCE) et la Cour européenne des droits de l'homme (CEDH) dont les décisions ont obligé à limiter la période de rétention des données et ont mis des obstacles à l'échange transatlantique des données [34].

32. Cour des comptes, *Référé sur les interceptions judiciaires et la Plateforme nationale des interceptions judiciaires*, 18 février 2016, p. 4.
33. http://www.presse.justice.gouv.fr/communiques-de-presse-10095/archives-des-communiques-de-2017-12858/la-plateforme-nationale-des-interceptions-judiciaires-en-chiffres-30997.html Consulté le 30 septembre 2019.
34. Voir sur ce point « Sigint intelligence transnational activities in France and Europe », compte rendu du colloque international organisé dans le cadre de l'ANR UTIC, les 24, 25 et 26 septembre 2018.

La seconde concerne l'accès administratif et non plus judiciaire aux données de connexion. On peut lire cette demande dans un mouvement plus général par lequel les services de renseignement cherchent à s'affranchir, au nom de l'urgence antiterroriste, des contrôles extérieurs qu'ils considèrent entraver leur action. Plus prosaïquement, cela relève également en France du faible nombre d'agents habilités à mener des procédures judiciaires par rapport à ceux qui ne le sont pas. Dans un service comme la DGSI, les premiers sont minoritaires. Ils sont pourtant les seuls à pouvoir agir sous le mandat d'un juge, afin d'exécuter toutes les demandes décrites ci-dessus. Leur multiplication rend donc le travail plus difficile (ils décrivent un sentiment de « saturation ») et souhaitent que ces tâches assez routinières puissent être partagées avec leurs homologues sans habilitations judiciaires.

À en juger par les évolutions législatives récentes, il semble qu'ils aient eu gain de cause sur ces deux chantiers, en France, en Grande-Bretagne et dans d'autres pays européens.

À la lecture de ce qui précède, on perçoit que les services de renseignement intérieur ont bien entendu adapté leurs pratiques aux évolutions technologiques de la société. Pour autant, ils n'ont pas bouleversé leurs logiques de travail. Ceci s'explique aisément. Si la plupart des services étudiés ont connu des augmentations de leurs effectifs et renforcé leurs sections dédiées à la violence politique à référence islamique, leurs recrutements ne concernent qu'à la marge des spécialistes de la technologie. Ils continuent pour l'essentiel à intégrer dans leurs rangs des policiers, des agents et des analystes dont les compétences correspondent aux métiers traditionnels du renseignement. Les savoir-faire en matière de traitement des sources humaines (les informateurs), de filatures ou d'interrogatoire continuent à être déterminants. Quitte d'ailleurs à sous-traiter les tâches les plus techniques. Ainsi, en France, les analyses de géolocalisation sont-elles confiées à des entreprises privées habilitées, qui examinent les données issues des réquisitions judiciaires et remettent ensuite des rapports aux agents du renseignement. En ce sens, les données numériques viennent nourrir des modes de raisonnement et des pratiques institutionnelles constituées sur la longue durée. Ils partent toujours d'un individu qu'ils suspectent et remontent patiemment son réseau de relations, afin d'identifier d'éventuels complices, de reconstituer des organigrammes, d'assigner des responsabilités à chacun. Ceci vaut bien entendu lorsqu'un délit ou un crime a été commis (un attentat, un départ en Syrie), mais également de manière préventive. L'essentiel du travail consiste ainsi à surveiller des réseaux d'individus et à accumuler sur eux le plus d'informations possibles (contacts, déplacements, propos et comportements).

Ce sens pratique des services de renseignement intérieur explique d'ailleurs qu'ils puissent facilement coopérer à l'échelle transnationale. Ceci ne

veut pas dire que cette coopération soit nécessairement harmonieuse. Il existe des liens privilégiés ou des inimitiés entre certains services liés à leur histoire. Ils peuvent également avoir des désaccords sur certaines questions. La situation Basque a ainsi été longtemps un sujet de discorde entre Français et Espagnols, celle de la guerre civile algérienne entre Français et Britanniques. Mais concernant la violence politique à référence islamique, il semble que se soit établi une sorte de consensus et ils échangent volontiers. Comme le signale un agent « on parle le même langage » (entretien, avril 2015). La proximité de pratiques et d'analyses facilite ainsi les échanges au-delà des frontières. Elle permet également la possibilité d'une certaine réciprocité dans les échanges, au moins entre les plus grands services. En effet, les données sur des individus et des groupes constituent un capital informationnel que les professionnels du renseignement n'aiment pas dilapider. Ils veulent être sûrs qu'une information donnée aura pour contrepartie une autre reçue, d'une égale utilité opérationnelle.

Ce premier pôle se distingue clairement du second pôle (2) qui regroupe les services recrutant notamment des militaires – ayant des capacités opérationnelles pour agir sur des terrains externes et usant de techniques d'espionnage. C'est le cas de la CIA et aussi d'autres services extérieurs, qui tendent davantage vers le renseignement humain (comme le MI6 britannique, l'ASIS australien). Certains organismes comme la DGSE française, le CNI espagnol et le BND allemand partagent les mêmes caractéristiques mais il faut signaler qu'ils ont développé ces dernières années des capacités importantes en matière d'interceptions de données dans des départements spécifiques qui sont dédiés à l'interception des données numériques à des fins de surveillance des réseaux sociaux. Ainsi, après 2008, la DGSE a-t-elle développé une ambitieuse politique en la matière, avec le renforcement de sa direction technique. Entre 2008 et 2013, elle bénéficie d'un plan d'investissement de 700 millions d'euros et de l'embauche de 600 personnes (notamment des ingénieurs télécom), qui lui permet d'intercepter les communications transitant par les câbles sous-marins d'opérateurs français comme Orange ou Alcatel-Lucent [35]. Il en va de même pour le CNI espagnol, qui, à Conil de la Frontera, dispose d'une station de captation du câble sous-marin Columbus III reliant la Sicile à la Floride [36]. Ils restent en revanche sous la supervision générale des services extérieurs et de la défense, tout en traitant comme « clients » les services de renseignement intérieur qui peuvent leur adresser des demandes spécifiques. Ici aussi, si l'informatique sert avant tout à géolocaliser des cibles extérieures, à rester en contact avec ses agents à l'extérieur, à éventuellement conduire des drones armés sur

35. L'enquête du journaliste Vincent Jauvert est à ce jour l'une des plus complètes sur cet épisode. Voir https://www.nouvelobs.com/societe/20150625.OBS1569/exclusif-comment-la-france-ecoute-aussi-le-monde.html. Consulté le 9 mars 2019. Voir également Follorou J., *L'État secret*, Paris, Fayard, 2018.
36. Rueda F., *La Casa II. CNI: Agentes, operaciones secretas y acciones inconfesables de los espías españoles*, Roca Editorial, Madrid 2017.

un terrain particulier, l'apport des *big data* ne doit pas conduire à l'imprécision sur les cibles dans des opérations politiquement très coûteuses. L'approximation n'est pas vraiment permise. Il ne s'agit pas de s'en passer, mais elle n'est qu'un outil d'exploration car la responsabilité sur le terrain prime.

Le troisième pôle du diagramme (3) renvoie lui à l'émergence d'un ensemble autonome des services SIGINT-Internet. Il s'agit là au contraire d'agences spécifiques, sans agents opérationnels, mais qui fournissent aux autres services nationaux (intérieurs et extérieurs) les données satellitaires, hertziennes et numériques dont ils ont besoin. Ce pôle est constitué quasi exclusivement des *Five Eyes*. S'y ajoute aussi la FRA suédoise qui a plus ou moins rejoint les *Five Eyes* étant donné son rôle dans l'interception des câbles internet sous-marins et terrestres qui vont en Russie et qui en partent. C'est dans cet espace particulier que s'est développée l'idée que les formes traditionnelles de renseignement étaient inopérantes face à de petits groupes inconnus. Dès les années 2000, l'amiral John Poindexter, alors directeur du Information Awareness Office aux États-Unis, a évoqué un quadrillage informatique des données globales avec le repérage des cibles, non à partir des individus déjà connus, mais à partir des anomalies de comportements repérées au sein de logiques systémiques. Ceci a été appelé le repérage des signaux faibles où des collections d'individus qui ne se connaissent pas forcément entre eux, ont comme seule caractéristique commune de correspondre à un profil de risque spécifique. Appelé initialement *Total Information Awareness* lorsque Poindexter fut rappelé par ses anciens amis après 2001 et eut les moyens à disposition pour cette idée, le projet fut néanmoins écarté, mais la NSA, grâce à sa surpuissance en termes de personnel et de budget, va se lancer dans l'aventure en faisant contribuer le secteur privé, tant au niveau des contractants de logiciels de *data mining* qu'au niveau des *providers* de l'Internet (les GAFAM) et des sociétés de téléphonie [37].

Après les divulgations de Snowden sur ces pratiques et l'ambition qui les guidait, on sait que plusieurs services de renseignement dont le GCHQ britannique ont insisté sur le fait que la surveillance potentielle de tous n'était pas mise en pratique et qu'elle était calibrée sur de petits groupes en raison justement du relais nécessaire avec une surveillance humaine effective. D'autres services les ont suivis dans cette stratégie de recalibrage. Il semble donc que les services d'interception des communications sensibles veuillent obtenir des facilités juridiques pour entreprendre des surveillances à grande échelle de groupes potentiellement dangereux en jetant un « large filet » mais qu'ils refu-

37. Harris, S., *The watchers: The rise of America's surveillance state*, Penguin, Londres, 2010 ; Murray N., « Profiling in the age of total information awareness », *Race & Class*, vol. 52, n°2, 2010, pp. 3-24 ; Ericson R., Haggerty K. (dir.), *The new politics of surveillance and visibility*, University of Toronto Press, Toronto, 2006.

sent en même temps l'idée d'un raisonnement algorithmique. Ce sont plutôt les services de surveillance financière ou plus récemment ceux du contrôle en amont des personnes autorisées à traverser les frontières, c'est-à-dire les nouveaux entrants dans le système, qui se targuent de pouvoir gérer de larges quantités d'information ou de personnes en utilisant les approches des signaux faibles car les coûts des faux positifs, sont, nous disent-ils, moins importants pour les personnes suspectées.

La construction sociologique d'un espace transnational du renseignement permet ainsi de regrouper les services de différents pays en fonction de la proximité structurelle du type d'objectif et des savoir-faire qu'ils emploient tout en visualisant les espaces distinctifs entre les services d'un même pays, contrastant ainsi avec nombre de représentations fondées sur une représentation territoriale nationale. Comme le montrent les visualisations issues de l'ACM, les discours habituels sur la confiance réciproque n'opèrent qu'entre agences ayant des positions structurelles identiques. En effet l'émergence finalement assez banale historiquement de deux des trois pôles autour de la frontière entre l'interne et l'externe n'est réellement perturbée que dans la mesure où le pôle des agences Sigint-Internet prend à son tour une place considérable dans la définition des données à partir de ses propres performances et grâce à un appui des hommes politiques à leurs initiatives, en grande partie corrélé avec un discours préventif et prédictif. C'est là où la transformation par l'informatisation et le recours au numérique de *qui* produit, échange et analyse les données, s'est surajouté, dans les années 2000, à l'arc de tension qui existait déjà entre les professionnels des services recrutés chez les militaires et ceux recrutés chez les policiers, lorsque la fin de la bipolarité a remis en cause les règles de bases qui avaient été données pour le monde de l'espionnage et du contre-espionnage.

Ces trois pôles s'autonomisent dans les pratiques des impératifs de fusion, homogénéisation ou stricte complémentarité qui leur sont demandées par les hommes politiques et les plus politiques de leurs supérieurs hiérarchiques. Mais ils n'échappent pas à leur emprise *via* les choix en termes budgétaires et de personnel, et c'est aussi dans les pays qui ont les plus fortes structures de coordination que cet effet est le moins visible. Ainsi, au Royaume Uni, le rôle du *Joint Intelligence Committee* est typiquement de maintenir une forte cohésion pour éviter ces jeux transnationaux, mais dans d'autres pays, ils sont au contraire encouragés comme l'a montré le rapport Feinstein afin de concentrer l'opacité des actions sur un service, souvent extérieur, le moins supervisé [38]. Nous avons évoqué ailleurs ce phénomène d'interaction dynamique où les échecs des uns constituent des conditions de félicité des autres. C'est ce qui s'est passé lorsque l'échec de la politique de torture de la CIA et de ses com-

38. United States Senate Select Committee on Intelligence, Committee Study of the Central Intelligence Agency's Detention and Interrogation Program, décembre 2014.

plices a délégitimé le recours au service dans les politiques de contre-terrorisme offensif [39]. Ceci a donné à l'armée régulière – *via* sa propre politique des drones –, et surtout à la NSA – avec son modèle d'action à distance, fondé sur le repérage algorithmique des anomalies de comportements – une position prééminente. Il est donc clair que les évolutions d'un sous ensemble spécifique, ici celui des services extérieurs, dont les stratégies soulèvent une réprobation internationale, ont eu un impact sur les décisions de renforcer les services SIGINT-Internet en leur donnant les moyens supplémentaires qu'ils réclamaient depuis longtemps.

***

Quels sont les résultats de notre analyse ? Tout d'abord qu'il n'existe nulle part un monde homogène (ou communauté) du renseignement où les services nationaux seraient complémentaires et où les frontières de leurs missions seraient clairement délimitées par le droit ou l'autorité politique. L'illusion d'un monde unique du renseignement uni par des techniques communes de surveillance changeant le sens de la sécurité (et l'entrainant globalement vers la spéculation) ne résiste pas à l'analyse des pratiques constitutives des acteurs et à la mise en sens qu'ils font des données. Les logiques d'action traversent, transgressent la distinction entre l'interne et l'externe, le national et l'étranger. L'apparente unité d'une communauté de renseignement national doit donc être patiemment déconstruite pour mettre en avant les relations constitutives qui existent entre des pôles différents en termes d'agences qui construisent les données de renseignement à des fins différentes, qui négocient entre elles et avec les hommes politiques quelles sont les approches les plus adaptées. Celles-ci entrent souvent en compétition entre elles, non à l'intérieur d'un champ national, mais à l'intérieur d'un espace transnational où les solidarités se font entre savoir-faire plus ou moins identiques, même s'il est lui-même hiérarchisé [40].

Les logiques distinctives entre services ne sont pas une pathologie, mais la structure même du jeu du renseignement dans des régimes démocratiques, et certaines tentatives de faire fusionner les services peuvent non seulement générer de l'inefficacité en déstabilisant les savoir-faire initiaux, mais aussi créer des structures trop puissantes en termes de traduction des données en fonction de certaines fins particulières, et par là mettre à mal la pluralité des interprétations et la valeur des discussions. Parler de ces logiques distinctives n'est dès lors pas un retour à l'image d'une « guerre des services » mais à une compréhension plus profonde des pratiques, au-delà des organigrammes qui

39. Bigo D., Guittet E., « The Quest for Absolution and Immunity. Justifying past and future torture in the name of democracy », dans Guild E., Bigo D. et M. Gibney (dir.), *Extraordinary Rendition…*, *op. cit.*, pp. 202-229.
40. Il suffit par exemple de penser que la NSA emploie plus de personnel que l'ensemble des services européens réunis.

sont donnés à voir par les organes politiques ou les agences de communication. Ces écarts entre services se reproduisent aussi en interne selon les critères de recrutement et les socialisations qui sont privilégiées. Certains ont opté pour de fortes homogénéités, en ne faisant confiance qu'à un type de métier, voire une seule école de formation, afin de constituer des solidarités, alors que d'autres veulent remplir la diversité des missions en choisissant des personnes qui ont des caractéristiques différentes en termes de formation, de genre, de gestion des pratiques de violence et d'usage des technologies du numérique. Un ingénieur réseau et un policier n'ont à l'évidence pas le même rapport au numérique, pas plus que ne se confondent celui du simple usager, du concepteur de logiciels ou de quelqu'un qui va créer des profils sur base d'algorithmes. Il en va de même entre ces derniers qui construisent des populations de catégories cibles et ceux qui pour remplir la même mission, se spécialisent dans l'établissement de dossiers individuels ou d'organisations et accordent une importance clé à la psychologie des individus et leurs trajectoires précises. Tous ceux-ci se vivent plus comme des analystes que comme des combattants, alors que ce n'est pas le cas de ceux qui vont utiliser des moyens coercitifs sur un terrain étranger. Les formations, les ressources des services, la légitimité de leur type d'action restent donc des ressources ou des capitaux inégalement répartis entre les acteurs intéressés au renseignement.

De l'ensemble des entretiens recueillis, il ressort néanmoins que l'utilisation des techniques numériques est mise au service, soit d'un cadre traditionnel de raisonnement indiciel et d'une relation aux preuves nécessaire pour le judiciaire, soit joue pour faire accepter un raisonnement préventif et prédictif. Les mécanismes de raisonnement propres à chaque univers, militaire, policier, ou communicationnel et les acteurs qui les portent sont alors bien plus importants que la technologie. Pour le dire autrement, ce qui joue alors est moins l'informatique en tant que telle, que l'entrée des informaticiens dans les cercles du renseignement et la manière dont ils posent les problèmes en amont de la technologie. C'est pourquoi l'entrée de la technologie ne doit pas être surestimée (comme le font certaines interprétations philosophiques). Elle ne nous dit rien de ses effets sur les pratiques. Elle peut simplement accélérer le croisement de données en lieu et place des anciens dossiers de papier mais sans bouleverser les logiques de travail. Elle peut intervenir comme régulation technique des bases de données et de leur interopérabilité et imposer certaines caractéristiques aux données, en particulier si elles ont comme objectif d'être échangées régulièrement et en grandes quantités. Elle peut enfin devenir plus significative si des départements spécifiques se créent au sein des services militaires ou policiers avec des tâches d'identification qui sont supervisées par ces acteurs techniques. Des conflits de dispositions peuvent apparaître, et au-delà, des tensions récurrentes sur la performativité des données. En effet, il n'est pas rare que dans les univers qui dépendaient déjà auparavant des données et d'une information non numérique, l'introduction de techniques, y compris

sophistiquées, ne change pas les modes de raisonnement. Il faut du temps pour que les intérêts des professionnels de ces techniques numériques réussissent à surajouter leurs propres intérêts aux intérêts traditionnels des acteurs du champ. Néanmoins, lorsque les ingénieurs réseaux, les analystes de données, les constructeurs de plateformes d'intégration, les spécialistes de langage et codes informatiques, les cryptologistes, les mathématiciens qui créent et/ou combinent des algorithmes jouant sur la reconnaissance de signaux faibles dans des séries longues, les entreprises privées qui emploient ces individus et vendent des produits et des services, viennent en force peupler des univers qui auparavant étaient composés quasi exclusivement de policiers, de gendarmes, de militaires, de spécialistes du renseignement interne ou externe, de gardes-frontières, ils modifient les règles du jeu. Et en changeant certaines règles et certaines habitudes, ils finissent par changer les dispositions pertinentes et exigibles, en particulier là où le monde privé des contractants est en bonne relation avec les agents publics des services. C'est sans doute là qu'est la plus-value des travaux sur la gouvernance des données que nous avons critiquée plus haut. Ils donnent à voir des tendances probables si ces derniers agents deviennent dominants dans le champ transnational des services de renseignements. Mais pour l'instant, ils n'en demeurent que des prétendants, et c'est la marge la moins légitime à l'intérieur du champ, les agents aux frontières et les acteurs du contrôle financier qui cherchent à visibiliser leurs approches dans les medias et auprès des chercheurs, pour se faire reconnaitre auprès des hauts responsables des services et de certains cercles proches des gouvernants de chaque pays.

Les enjeux propres à ces nouveaux professionnels de l'information sensible se sont donc imposés de manière non homogène dans les différents univers du renseignement, mais de manière transversale, ils ont tout particulièrement séduit ceux qui se voulaient de plus en plus préventifs et prédictifs, promouvant comme nous l'avons vu une vision selon laquelle seules les potentialités et possibilités que le digital apporte dans ces domaines, peuvent mettre en adéquation les *desiderata* des hommes politiques, les peurs des populations et les intérêts des appareils de sécurité engagés dans la gestion des populations à distance. Cette prétendue adéquation reste à discuter. Elle devient néanmoins un élément constitutif du monde du renseignement et de la surveillance, en reliant la haute politique et le quotidien et en redéfinissant différemment ce qui était nommé la sécurité nationale.