IRSEM
INSTITUT DE RECHERCHE STRATÉGIQUE DE L'ÉCOLE MILITAIRE

Septembre 2022

COMPRENDRE LE MOYEN-ORIENT PAR LA DONNÉE

TECHNOLOGIES NUMÉRIQUES ET ACQUISITION DE LA CONNAISSANCE DANS LA RÉGION AFRIQUE DU NORD / MOYEN-ORIENT

COL Olivier Passot

Chercheur associé à l'IRSEM

ÉTUDE – n° 98

MINISTÈRE DES ARMÉES
Liberté
Égalité
Fraternité

IRSEM
INSTITUT DE RECHERCHE STRATÉGIQUE DE L'ÉCOLE MILITAIRE

COMPRENDRE LE MOYEN-ORIENT PAR LA DONNÉE

TECHNOLOGIES NUMÉRIQUES ET ACQUISITION DE LA CONNAISSANCE DANS LA RÉGION AFRIQUE DU NORD / MOYEN-ORIENT

COL Olivier Passot

Chercheur associé à l'IRSEM

Pour citer cette étude
Olivier Passot, *Comprendre le Moyen-Orient par la donnée – Technologies numériques et acquisition de la connaissance dans la région Afrique du Nord / Moyen-Orient*, Étude 98, IRSEM, septembre 2022.

Dépôt légal
ISSN : 2268-3194
ISBN : 978-2-11-167760-9

DERNIÈRES ÉTUDES DE L'IRSEM

97. *La Russie au Mali : une présence bicéphale*
Maxime AUDINET et Emmanuel DREYFUS

96. *La singularité du métier militaire : persistances et nouveautés – Pourquoi défendre un modèle de singularité ?*
Clément SORBETS

95. *L'armée, les Français et la crise sanitaire : une enquête inédite*
Anne MUXEL, Florian OPILLARD et Angélique PALLE

94. *L'extrémisme islamiste au nord du Mozambique : terrorisme et insécurité à Cabo Delgado*
Régio CONRADO

93. *La latence nucléaire du Japon : un levier diplomatique à double usage ?*
Timothée ALBESSARD

92. *Le régime milicien iranien en Irak – Les milices chiites pro-iraniennes à la conquête de l'État*
Arthur QUESNAY

91. *Facing a pandemic: African armies and the fight against COVID-19*
Anne-Laure MAHÉ and Nina WILÉN (eds)

90. *L'intervention française au Sahel et l'évolution de la doctrine de contre-insurrection*
Michael SHURKIN

89. *Observatoire de la génération Z*
Anne MUXEL

88. *Le ministère des Armées face à l'agenda Femmes, paix et sécurité – Évolution des approches et défis de mise en œuvre*
Camille BOUTRON

ÉQUIPE

Directeur
Jean-Baptiste JEANGÈNE VILMER

Directrice adjointe
Marjorie VANBAELINGHEM

Directeur scientifique
Jean-Vincent HOLEINDRE

Secrétaire générale
Caroline VERSTAPPEN

Éditrice
Chantal DUKERS

Retrouvez l'IRSEM sur les réseaux sociaux :

@ https//www.irsem.fr

@IRSEM1

AVERTISSEMENT : l'IRSEM a vocation à contribuer au débat public sur les questions de défense et de sécurité. Ses publications n'engagent que leurs auteurs et ne constituent en aucune manière une position officielle du ministère des Armées.

© 2022 Institut de recherche stratégique de l'École militaire (IRSEM).

PRÉSENTATION DE L'IRSEM

L'Institut de recherche stratégique de l'École militaire (IRSEM), créé en 2009, appartient au ministère des Armées. Composé d'une cinquantaine de personnes, civiles et militaires, dont la plupart sont titulaires d'un doctorat, il est le principal centre de recherche en études sur la guerre (*War Studies*) dans le monde francophone. En plus de conduire de la recherche interne (au profit du ministère) et externe (à destination de la communauté scientifique) sur les questions de défense et de sécurité, l'IRSEM apporte un soutien aux jeunes chercheurs (la « relève stratégique ») et contribue à l'enseignement militaire supérieur et au débat public.
L'équipe de recherche est répartie en six domaines :

- Le domaine Espace euratlantique – Russie analyse les évolutions stratégiques et géopolitiques en Amérique du Nord, en Europe, en Russie et dans l'espace eurasiatique qui comprend l'Europe orientale (Moldavie, Ukraine, Biélorussie), le Caucase du Sud (Arménie, Géorgie, Azerbaïdjan) et les cinq pays d'Asie centrale. Il s'intéresse plus particulièrement à la compétition de puissances dans cette zone, aux évolutions du rôle de l'OTAN, à la sécurité maritime et aux stratégies d'influence.
- Le domaine Afrique – Asie – Moyen-Orient analyse les évolutions stratégiques et géopolitiques en Afrique, Asie et Moyen-Orient, autour des axes transversaux suivants : autoritarisme politique et libéralisation économique dans les pays émergents ; rôle et place des armées et des appareils de sécurité dans le fonctionnement des États et des sociétés ; enjeux stratégiques et de sécurité régionale ; idéologies, nationalismes et recomposition des équilibres interétatiques régionaux.
- Le domaine Armement et économie de défense s'intéresse aux questions économiques liées à la défense et, plus largement, a vocation à traiter des questions stratégiques résultant des développements technologiques, des problématiques d'accès aux ressources naturelles et de celles liées aux enjeux environnementaux. Les travaux de recherche du domaine s'appuient sur une approche pluridisciplinaire, à la fois qualitative et quantitative, qui mobilise des champs scientifiques variés : économie de défense, histoire des technologies, géographie.

• Le domaine Défense et société est à l'interface des problématiques spécifiques au monde militaire et des évolutions sociétales auxquelles celui-ci est confronté. Les dimensions privilégiées sont les suivantes : lien entre la société civile et les armées, sociologie du personnel militaire, intégration des femmes dans les conflits armés, relations entre pouvoir politique et institution militaire, renouvellement des formes d'engagement, socialisation et intégration de la jeunesse, montée des radicalités. Outre ses activités de recherche, le domaine Défense et société entend aussi promouvoir les questions de défense au sein de la société civile, auprès de l'ensemble de ses acteurs, y compris dans le champ académique.
• Le domaine Stratégies, normes et doctrines a pour objet l'étude des conflits armés contemporains, en particulier sous leurs aspects politiques, militaires, juridiques et philosophiques. Les axes de recherche développés dans les productions et événements réalisés portent sur le droit international, en particulier sous l'angle des enjeux technologiques (cyber, intelligence artificielle, robotique), les doctrines de dissuasion, la maîtrise des armements avec la lutte contre la prolifération et le désarmement nucléaires. Les transformations des relations internationales et leurs enjeux de puissance et de sécurité ainsi que la philosophie de la guerre et de la paix font également partie du champ d'étude.
• Le domaine Renseignement, anticipation et menaces hybrides mène des recherches portant sur la fonction stratégique « connaissance et anticipation » mise en avant par le Livre blanc de la défense depuis 2008. Ce programme a donc d'abord pour ambition de contribuer à une compréhension plus fine du renseignement entendu dans son acception la plus large (c'est-à-dire à la fois comme information, processus, activité et organisation) ; il aspire ensuite à concourir à la consolidation des démarches analytiques, notamment dans le champ de l'anticipation ; enfin, il travaille sur les différentes dimensions de la guerre dite « hybride », en particulier les manipulations de l'information. Le domaine contribue du reste au renforcement du caractère hybride de l'IRSEM en diffusant des notes se situant à l'intersection de la recherche académique et de l'analyse de renseignement en sources ouvertes.

BIOGRAPHIE

Issu des Troupes de marine, le colonel Olivier Passot a servi dans des unités opérationnelles, à la formation des officiers et en état-major. Sa deuxième partie de carrière a été principalement orientée vers l'international au sein des armées et du ministère (coopération, renseignement et questions stratégiques). Il a effectué de nombreuses missions à l'étranger, notamment au Moyen-Orient. Il a été directeur du domaine « Pensée stratégique » à l'IRSEM de 2017 à 2018. Il y est aujourd'hui chercheur associé.

SOMMAIRE

RÉSUMÉ

Les technologies liées au recueil et au traitement de la donnée ouvrent des perspectives considérables au regard de la connaissance et du renseignement. Elles sont capables de percer des environnements difficilement perméables, à condition que les données collectées puissent être analysées. Or la question de la perméabilité d'un espace spécifique à ces nouveaux usages a été peu étudiée. La région Afrique du Nord / Moyen-Orient (ANMO), souvent considérée comme compliquée dans l'imaginaire occidental, peut-elle être décryptée plus facilement grâce à cette transformation technologique ?

Cet espace présente une exposition contrastée à la donnée : d'un côté, la collecte est limitée par de multiples barrières (contrôle politique et social, insécurité, codes culturels) ; de l'autre, les individus sont de plus en plus exposés à la surveillance numérique en raison d'une régulation encore faible, tandis que les comportements se digitalisent très vite. De fait, des acteurs publics et privés toujours plus nombreux collectent et analysent des *data* pour informer, investiguer et tracer, transformant le terrain de la connaissance en un espace concurrentiel. Si ces technologies offrent des opportunités à certains gouvernements de la région ANMO, notamment dans l'exercice de leurs missions régaliennes, elles représentent d'importants défis pour la majorité d'entre eux. L'acquisition des compétences, le contrôle des données et de la souveraineté nécessiteront des investissements très importants dans un proche avenir. Les États qui n'y parviendront pas risquent d'être concurrencés par les nouveaux acteurs de la donnée.

INTRODUCTION

Correspondant au MENA (Middle East and North Africa) anglo-américain, qui s'étend du Maroc à l'Iran et rassemble près de 400 millions d'habitants, la région Afrique du Nord / Moyen-Orient (ANMO) est, au-delà des allégories, un véritable nœud d'enjeux géopolitiques. Elle recouvre une grande diversité, sinon disparité, de sphères culturelles, linguistiques ou religieuses, réparties en une vingtaine d'États aux régimes variés : démocraties parlementaires, républiques théocratiques, monarchie de droit divin, voire parfois absence d'État effectif.

À cette diversité politique et culturelle fait écho une diversité de crises : sécuritaires, migratoires, énergétiques... Comment recueillir, dans ces conditions, la connaissance nécessaire à la compréhension d'une région aussi complexe et disparate, afin d'en tirer les enseignements stratégiques utiles ?

Les nouvelles technologies, qui produisent des masses de données numériques inédites, peuvent constituer un élément de réponse. En effet, la croissance exponentielle du volume de données numériques produites, rendue possible par les progrès informatiques (processeurs, stockage, *cloudcomputing*, etc.), par la généralisation de l'internet haut débit et des objets connectés, ainsi que d'autres technologies très bon marché, démultiplie les possibilités d'analyse et d'accumulation de la connaissance. Cette révolution du *big data* touche aussi la région ANMO, et, comme ailleurs dans le monde, les différents acteurs du marché de l'information doivent adapter leurs modes de fonctionnement au règne des mégadonnées. Ces dernières présentent nombre de nouvelles opportunités pour la compréhension et l'analyse de milieux stratégiques, mais apportent également leur lot de défis et nouveaux enjeux.

Ainsi, la donnée telle qu'elle sera traitée dans cette étude est une « information numérique et codée, lisible par une machine en vue de son enregistrement, traitement, conservation et communication[1] ». Prise individuellement, l'information contenue

1. Éric Pérès, « Les données numériques : un enjeu d'éducation et de citoyenneté », avis du Conseil économique, social et environnemental, janvier 2015.

dans chaque donnée est brute et n'a pas grande valeur mais lorsque les données sont collectées en très grand nombre (*big data*), puis traitées selon des processus informatiques et statistiques, elles peuvent produire des informations quasiment illimitées. Le traitement et l'exploitation de ces masses de données peuvent ainsi servir à la compréhension[2] de certains événements, phénomènes ou encore dynamiques. C'est notamment le recueil et l'exploitation d'informations dites « stratégiques » que nous allons tenter d'aborder ici.

La notion d'information stratégique, souvent utilisée, mérite d'être précisée. On se référera pour cela aux deux concepts sous-jacents de « stratégie » et de « décision stratégique », définis par Hervé Coutau-Bégarie : la stratégie est une « dialectique des intelligences, dans un milieu conflictuel » ; quant à la décision stratégique, elle repose sur une volonté d'agir mais aussi sur « la capacité de maîtriser une situation »[3]. Pour Coutau-Bégarie, la décision prise sous contrainte requiert de l'intelligence (celle du chef, ou – peut-être – celle que procure le renseignement) ainsi qu'une claire appréciation de situation. Ces deux conditions ne peuvent être remplies sans disposer d'informations spécifiques et à haute valeur ajoutée, car l'intelligence qui préside à la décision stratégique « se heurte à une intelligence antagoniste[4] ». Dans ce contexte, l'information stratégique est celle qui procure un avantage concurrentiel sur un terrain d'affrontement (politique, militaire, économique) ; par extension, c'est une information qui permet au décideur de se protéger des menaces et des risques alors qu'il évolue dans un environnement dangereux ou complexe.

2. En s'inspirant de l'approche britannique, on la définira comme la « perception et l'interprétation d'une situation particulière afin d'en appréhender le contexte, les ressorts internes et les perspectives nécessaires à la prise de décision » (Ministère de la Défense britannique, *Joint Doctrine Publication 2-00, Understanding and Intelligence Support to Joint Operations,* 2011).

3. Hervé Coutau-Bégarie, *Traité de stratégie*, Paris, Economica, 2002, p. 74-75. Coutau-Bégarie s'appuie sur les définitions de Beaufre et de Freund, qu'il complète.

4. *Ibid*., p. 76.

Ainsi, les nouvelles technologies de traitement des données numériques sont essentielles au travail du renseignement, lequel, générant des connaissances exploitables pour l'action[5], est incontournable dans le processus de prise de décision stratégique. Le renseignement intègre régulièrement des innovations techniques qui augmentent ses capacités. Cependant, avec les technologies de traitement de données, il semble qu'on ait affaire à un changement d'échelle dans la collecte et la sophistication, comme en témoignent par exemple les révélations du lanceur d'alerte Edward Snowden qui, en 2013, a levé le voile sur le système de surveillance massif déployé par la National Security Agency (NSA) américaine. Les chercheurs commencent ainsi à étudier la manière dont les grandes agences de renseignement intègrent l'usage des données massives[6]. Ils documentent les défis techniques, humains et organisationnels que cette appropriation implique pour les acteurs du renseignement (Zegat[7], Moses et Chan[8]). Beaucoup de travaux portent sur l'apport du renseignement d'origine sources ouvertes (en anglais *open-source intelligence*, abrégé en OSINT)[9] ou de l'analyse des médias sociaux (Omand[10]).

Désormais, ces technologies sont capables de percer des environnements difficilement perméables, pour peu qu'on puisse

5. Jerry H. Ratcliffe, *Intelligence-Led Policing*, Cullompton, Devon, Willan, 2008.

6. On renverra tout particulièrement à Damien Van Puyvelde, chercheur associé à l'IRSEM : Damien Van Puyvelde, Stephen Coulthart et Shahriar Hossain, « Beyond the buzzword: big data and national security decision-making », *International Affairs*, 93:6, Oxford, Oxford University Press, 2017.

7. Amy Zegar, *Spies, Lies and Algorithms: The History and Future of American Intelligence*, Princeton, Princeton University Press, 2022.

8. Lyria Bennett Moses et Janet Chan, « Using Big Data for Legal and Law Enforcement Decisions: Testing the new Tools », *University of New South Wales Law Journal*, 37:2, 2014, p. 643-678.

9. Mark M. Lowenthal, « Open-Source Intelligence: New Myths, New Realities », dans Roger Z. George et Robert D. Kline (eds), *Intelligence and the National Security Strategist: Enduring Issues and Challenges*, Washington, DC, National Defense University Press, 2004, p. 273-278.

10. Sir David Omand, Jamie Bartlett et Carl Miller, « Introducing Social Media Intelligence (SOCMINT) », *Intelligence and National Security*, 27:6, 2012, p. 801-823.

analyser les données collectées. Or, la question de la perméabilité d'un espace spécifique à ces nouveaux usages n'a pas été vraiment abordée : comment évaluer le niveau de numérisation d'un espace aussi disparate que la région ANMO, dont la complexité géopolitique semble parfois confiner à l'opacité ? Plus précisément, quelles y sont les opportunités offertes par le *big data* dans le cadre du traitement d'informations stratégiques ?

En effet, dans quelle mesure ce déferlement soudain et massif de données a-t-il contribué à numériser cette région, bien souvent qualifiée de « compliquée[11] » par l'imaginaire collectif occidental ? En quoi cette numérisation pourrait-elle servir à améliorer la compréhension de cet environnement ? Cette promesse de la connaissance par la technologie doit-elle conduire les appareils de renseignement à adapter leur dispositif et leurs méthodes, dans cette région du monde ?

Nous présenterons tout d'abord un éventail de techniques et d'outils, liés à la science des données, qui permettent d'améliorer la connaissance et qui sont déjà utilisés dans la région ANMO. Nous tenterons d'évaluer le niveau d'exposition de cet espace à la digitalisation, à la collecte des données et à la surveillance numérique. Nous décrirons les acteurs qui interviennent sur le marché de l'information et de la connaissance, en recourant aux outils numériques pour accroître leurs performances (administrations, entreprises, médias, centres de recherche, individus eux-mêmes).

Nous présenterons enfin les défis auxquels sont confrontés les gouvernements de la région, face à cette nouvelle donne informationnelle. Si l'étude est spécifiquement orientée vers la région ANMO, certains développements ont tendance à dépasser ce cadre géographique ; de fait, la relation entre les technologies numériques et l'acquisition d'informations stratégiques, que cette étude interroge, peut difficilement être circonscrite à une seule région du monde.

11. Parmi tant d'autres, on rappellera la fameuse phrase du général de Gaulle : « Vers l'Orient compliqué, je volais avec des idées simples » (*Mémoires de guerre*, *L'Appel (1940-1942)*, Paris, Plon, 1954, p. 145).

I. LES OUTILS POUR COLLECTER LES DONNÉES

L'exploitation des données à des fins de connaissance est un phénomène récent dans la région ANMO, en raison d'une digitalisation restreinte jusqu'à la fin des années 2000. Depuis, les technologies numériques se diffusent vite, couvrant des domaines toujours plus étendus. Parmi les innombrables applications des données, certaines s'inscrivent dans le champ de l'information et du renseignement.

Nous en proposons ici une catégorisation en quatre familles, qui démultiplient toutes l'accès à la connaissance. La classification proposée est établie en fonction du but stratégique poursuivi par l'utilisateur, dans l'utilisation des données et des algorithmes. En schématisant, il s'agit des fonctions suivantes : informer, surveiller, investiguer, tracer[1].

INFORMER : COUVERTURE MÉDIATIQUE DES CONFLITS ARMÉS ET DES SITUATIONS DE CRISE

La plupart des grands conflits qui ont déchiré la région ANMO jusqu'au début des années 2000 (guerres israélo-arabes et guerres du Golfe) étaient de nature interétatique. Ils opposaient deux camps, de part et d'autre d'une ligne de front. Chaque camp était couvert par des journalistes accrédités. Aujourd'hui, les zones de crises sont contestées entre une multitude d'acteurs. La guerre du Liban (1975-1990), qui apparaissait comme une exception, est devenue la forme standard des affrontements : dimensions internes et externes, fronts mouvants, allégeances fluctuantes. Selon les critères pris en compte, la région ANMO compte environ dix conflits ouverts ou latents, dont les principaux sont : le conflit israélo-palestinien, israélo-libanais, les guerres en Irak, en Libye, en Syrie et au Yémen, ainsi que l'affrontement régional

1. Cette classification est imparfaite (il existe des superpositions et des duplications dans les usages). Elle se place dans la perspective de l'utilisateur et non dans celle des méthodes utilisées.

opposant l'Iran à plusieurs adversaires. La région connaît parallèlement de nombreux foyers de contestation interne. Vue de l'Occident, par des observateurs non aguerris, cette région peut sembler peu lisible, âpre à comprendre, avec ses « guerres sans fin[2] » auxquelles se mêlent rivalités régionales, affrontements ethniques et religieux ainsi que divers enjeux énergétiques et alimentaires. Toutefois, elle suscite un grand intérêt auprès de l'opinion publique, transposant parfois dans le débat sociétal occidental les passions antagonistes[3] autour de certains sujets.

Alors que les journalistes sont exposés à des risques croissants sur le terrain (assassinats, enlèvements, colère des populations), les agences de presse et les médias traditionnels réduisent le nombre de leurs correspondants. L'absence de couverture journalistique pose le problème de l'accès à une information neutre et documentée, d'autant que les représentations diplomatiques ne sont plus systématiquement assurées dans les pays en crise. La France, dont le réseau est l'un des plus ramifiés au monde, n'a plus d'ambassade ni de consulat dans trois pays de la zone ANMO[4].

Pour couvrir des zones dangereuses ou difficiles d'accès, les technologies liées à la donnée offrent des alternatives très intéressantes, sans supporter le risque d'avoir des correspondants sur le terrain. Ces techniques sont toutefois conditionnées à l'accès à internet (notamment par réseaux mobiles). Par exemple, la guerre en Syrie a été massivement suivie par des observateurs, blogueurs ou « journalistes-citoyens », tandis que les journalistes traditionnels peinaient à accéder aux zones de conflits. Ces nouveaux reporters jouent en général le rôle de sources primaires, au plus près des événements. Certains font plus : présents sur le terrain ou à distance, ils questionnent l'authenticité des contenus

2. L'expression de « guerres sans fin » a été employée par le président Biden pour justifier le retrait d'Afghanistan (Adresse à la nation du 31 août 2021). *Questions internationales* a également titré « Moyen-Orient : des guerres sans fin », 103-104, 13 octobre 2020.

3. Denis Sieffert, *Israel-Palestine, une passion française*, Paris, La Découverte, 2004.

4. La France n'entretient plus de représentation diplomatique permanente en Syrie, ni au Yémen, ni en Libye.

postés par l'analyse collaborative de données (*crowdsourcing*[5]). Ce travail de recoupement et de synthèse est devenu indispensable compte tenu de la profusion de données accessibles sur les réseaux sociaux. Un développement sur ces nouveaux acteurs figure dans la troisième partie.

SURVEILLER : LA DONNÉE COLLECTÉE DANS LE CIEL

Les images prises depuis le ciel, combinées aux techniques de positionnement par satellites, aux bases de données géospatiales (et à d'autres techniques encore) offrent des avantages considérables pour suivre en ligne et en temps réel des personnes, des véhicules et des événements. La géomatique regroupe les connaissances et les techniques destinées à la production et au traitement des données numériques décrivant des objets ou des phénomènes géoréférencés. Les données acquises par satellites, avions ou drones permettent de cartographier et d'observer des zones très étendues. Conjuguées avec la technologie GPS et les données émises par les téléphones mobiles, elles permettent de localiser des individus en temps réel avec une grande précision. Plusieurs sociétés privées ont développé des applications capables de localiser des individus, y compris dans des zones éloignées des centres urbains (Babel Street, X-Mode, Venntel…)[6]. Ces outils sont utilisés notamment par les responsables de sécurité (*risk managers*, *security officers*) qui opèrent pour le compte d'ONG, de compagnies pétrolières, sociétés minières, compagnies d'assurances... : applications de traçage GPS, système embarqué de navigation maritime[7], etc. Des sociétés technologiques se sont

5. *Crowdsourcing* peut se traduire, de manière plus stricte, par « externalisation à grande échelle » ou « production participative à grande échelle ». Ce point est étudié dans la troisième partie.

6. Ces sociétés utilisent des bases de données achetées auprès de *brokers* ou d'autres sociétés technologiques, qui détiennent des données personnelles à partir d'applications développées (applications de rencontre, de navigation, etc.).

7. Le système d'identification automatique (AIS) permet de suivre la navigation maritime de manière automatisée (transpondeurs radio, position GPS) et sécurisée (afin d'éviter les collisions entre autres).

même spécialisées dans la surveillance au profit des services de sécurité gouvernementaux, y compris pour localiser des individus à leur insu[8].

Les forces armées modernes disposent de plus en plus de capteurs, choisis en fonction de divers paramètres : missions à remplir, étendue de la zone d'opérations, cibles potentielles, niveau de menace. En mission de surveillance, ces capteurs sont le plus souvent embarqués sur des plateformes aéroportées, ce qui permet de couvrir de grandes étendues en fusionnant les informations collectées. Pour surveiller un théâtre d'opérations aussi étendu que le Sahel, l'armée française combine de multiples plateformes (drones MALE, avions légers de reconnaissance, avions de combat, satellites) qui ont des caractéristiques et des performances complémentaires (endurance, vitesse, emport de charge utile). Ces moyens démultiplient les capacités à « balayer » le champ de bataille et permettent de le cartographier numériquement avec précision. Les nouvelles technologies d'information et de communication peuvent mettre à jour en temps quasi réel la situation tactique. La numérisation multiplie la connaissance de l'environnement, garantissant « l'efficacité militaire tout en minimisant les menaces et les risques[9] ».

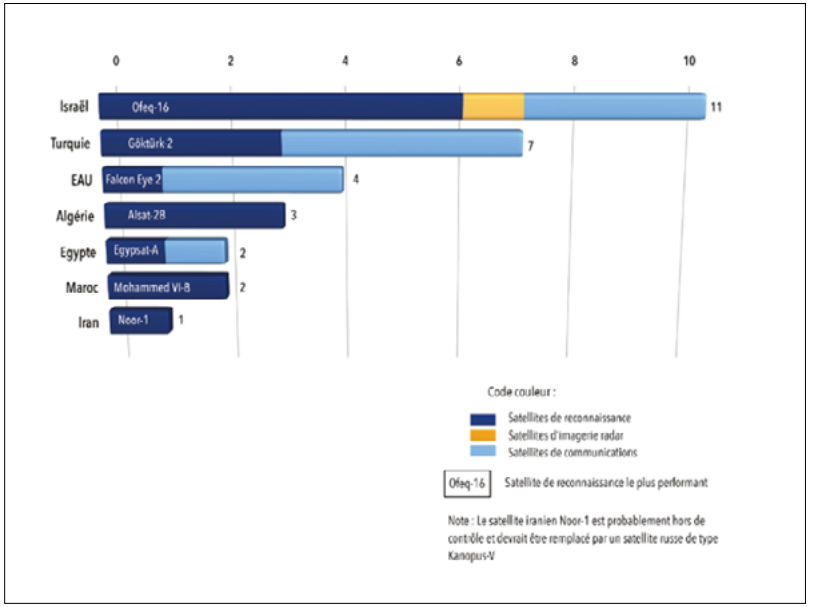
De plus en plus de pays de la zone ANMO accèdent aux plateformes de surveillance aérienne et à la numérisation du champ de bataille. Les avions de combat de dernière génération, qui équipent aujourd'hui plusieurs armées de l'air de la région ANMO, s'apparentent à des plateformes collectant des masses considérables de données, que seuls des algorithmes et

8. Sur son site, Babel Street prétend fournir des informations critiques à de nombreux gouvernements à travers le monde. Plusieurs agences gouvernementales feraient partie des clients (Carey Shenkman, Sharon Franklin, Greg Nojeim, Dhanaraj Thakur, « How Law Enforcement and Intelligence Agencies Are Buying Your Data from Brokers », Center for Democracy and Technology, décembre 2021).

9. Amaël Cattaruzza, Stéphane Taillat, « Les enjeux de la numérisation du champ de bataille », *Dynamiques internationales*, 13 juin 2018.

des intelligences artificielles peuvent traiter[10]. Les drones MALE, capables de surveiller des zones pendant 24 heures ou plus, sont de plus en plus répandus dans la région. La plupart des armées arabes du Golfe, d'Israël, d'Iran, du Maroc et de la Turquie en possèdent, et les équipent d'ailleurs, progressivement, de systèmes d'armes[11]. Une société émirienne a développé son premier avion dédié aux missions ISR[12].

Les États dotés de satellites militaires dans la région ANMO[13]



Les satellites, quant à eux, permettent de s'affranchir des contraintes liées aux espaces aériens nationaux et offrent une très

10. Thomas Schumacher, « F-35 & Big Data : épée de Damoclès pour la France et l'Europe », *Revue Défense Nationale*, 810, mai 2018, p. 35-40.

11. Khaled Hamadeh, « Drone Race in the Middle East », *Ashark Al-Awsat*, 30 janvier 2022.

12. La société Aquila Aerospace (filiale d'Edge Group) a développé le premier ISR émirien (*Intelligence Online*, 872, 10 mars 2021).

13. *Atlas stratégique de la Méditerranée et du Moyen-Orient*, Fondation méditerranéenne d'études stratégiques, 2022.

large couverture. Les satellites d'observation de dernière génération produisent des flux de données tellement considérables qu'ils rendent indispensable le recours à l'intelligence artificielle afin de traiter cette masse[14]. L'IA permet d'exploiter beaucoup plus efficacement les images recueillies et de gagner en vitesse de traitement. Sept pays de la zone ANMO sont déjà dotés de satellites militaires. Quatre disposent à la fois de capacités d'observation et de communication. L'Iran a lancé son premier satellite militaire d'observation en avril 2020, suivant ainsi l'Arabie, l'Égypte, le Maroc et le Qatar, qui ont déjà des programmes d'observation spatiale.

Les systèmes d'information géospatiale (SIG)[15] permettent d'appréhender les aspects géographiques d'un ensemble de données. Ils sont reliés à une base de données qu'ils interrogent ou analysent, et modélisent le résultat sous la forme d'une carte.

Les SIG sont utilisés dans de très nombreux domaines liés à la représentation de l'espace : prévisions démographiques, exploration pétrolière et minière, connaissances des ressources en eau, agriculture, météorologie, mobilité et transport. Naturellement, les SIG apportent une plus-value considérable au renseignement (renseignement géospatial, ou GEOINT), en agrégeant des données provenant de sources multiples qu'une IA peut filtrer ou fusionner à volonté.

Les images satellite, combinées aux données recueillies par d'autres capteurs (radars, caméras), permettent de cartographier des phénomènes dynamiques très précisément, avec des mises à jour régulières. En période de crise sanitaire, elles permettent par exemple de cartographier la propagation d'une pandémie ou les ressources disponibles pour y faire face.

Le recueil de données en temps réel fournit un véritable tableau de bord mis à jour au quotidien, grâce auquel l'utilisateur peut prendre des décisions plus pertinentes, en s'appuyant

14. Philippe Boulanger, « Géopolitique du Geospatial Intelligence dans le monde », *Stratégique*, 126-127, 2021, p. 35-49.

15. Plutôt que le terme GEOINT (*geospatial intelligence*), restreint au champ du renseignement, on fera référence aux systèmes d'information géospatiale.

sur des indicateurs géoréférencés. Prenons une ONG qui planifie une opération d'assistance à la population en Syrie, tout en n'ayant accès à une région que pendant une durée limitée. Grâce à l'analyse de données, elle identifiera les lieux et les horaires où elle pourra toucher le plus de monde possible. En recueillant les émissions GSM des utilisateurs de mobiles dans une région donnée, elle pourra dessiner une cartographie des densités humaines, en fonction des jours de la semaine, ou des heures de la journée. Les données géoréférencées ont d'innombrables usages qui concourent à optimiser des ressources comptées : suivre le trafic routier (à partir des signaux GPS émis par les voitures), l'activité aéroportuaire ou encore la densité d'une manifestation. En plus du temps réel, l'approche collaborative accroît l'efficacité de l'analyse.

Dans la région ANMO, de très nombreuses expériences sont en cours. On citera par exemple l'analyse des destructions en zone de guerre (Irak, Syrie, Yémen)[16], l'étude des rassemblements informels de réfugiés syriens au Liban, l'exploration pétrolière[17], l'évaluation de l'évaporation des eaux de la mer Morte, le suivi des phénomènes naturels (météo, invasion de criquets, etc.), la gestion du trafic routier, ou encore l'assainissement[18]. L'émirat de Dubaï met en place un système de transport intelligent, qui s'appuie sur des SIG ainsi que beaucoup d'infrastructures et de l'IA. Il prévoit que 25 % du transport public sera « autonome » à partir de 2030. Israël a investi aussi beaucoup dans la mobilité

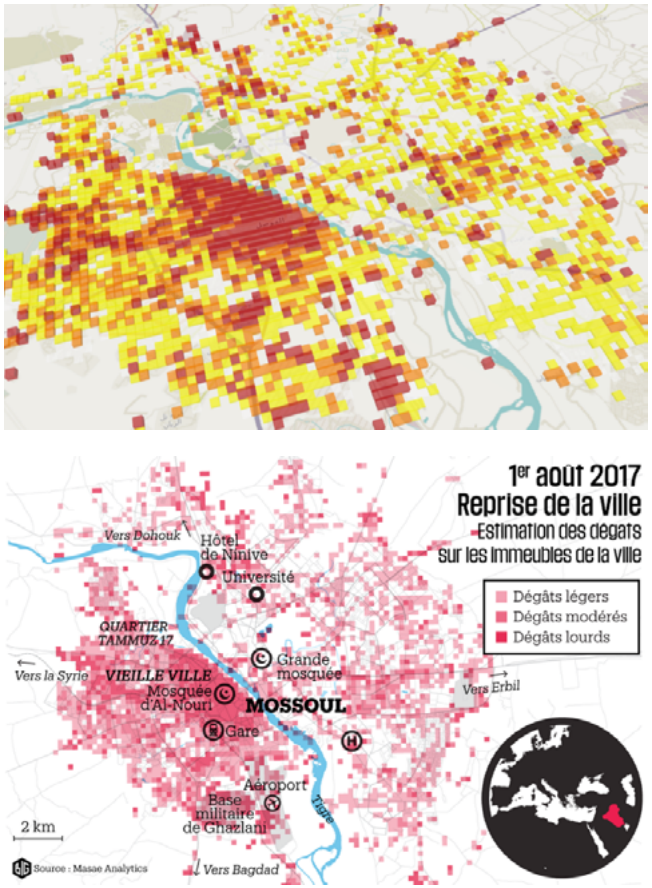
16. La start-up française MASAE utilise l'imagerie procurée par un radar à synthèse d'ouverture (RSO/ SAR), https://sar.masae-analytics.com/.

17. Les majors pétroliers utilisent le *big data* pour prédire le succès des opérations de forage : https://cyberorient.net/wp-content/uploads/sites/3/2017/10/CyberOrient_Vol_11_Iss_2_Allagui_Ayish.pdf.

18. La plateforme collaborative Octopus, développée par l'ONG Solidarités International, recense les zones de boues fécales et propose des outils pour l'assainissement, https://defishumanitaires.com/2019/04/23/octopus-la-premiere-plateforme-collaborative-qui-revolutionne-les-pratiques-humanitaires-en-situation-durgence/.

intelligente, grâce à une multitude de start-up innovantes et à des centres de recherche spécialisés[19].

À partir d'images aériennes prises des maisons détruites à Mossoul, la société MASAE modélise l'état de la ville



Source : MASAE analytics © OpenStreetMap contributors (Contains modified Copernicus Sentinel data 2017, processed by Masae Analytics).

19. Plusieurs centres de recherche sont spécialisés en matière de ville intelligente : Bar Ilan Center for Smart Cities (https://friends.org/smartcity), City Center à l'université de Tel-Aviv (https://urban.tau.ac.il/), entre autres.

INVESTIGUER : CIBLAGE D'INDIVIDUS OU D'ORGANISATIONS, LUTTE CONTRE LA CRIMINALITÉ (*LAW ENFORCEMENT*)

Contrairement à la fonction de surveillance, par laquelle on cherche à détecter un signal non conforme à un comportement ou un *pattern* attendu, la fonction d'investigation recherche les relations entre entités (*link analysis*) et classe les données pour cibler des catégories (*classification* et *clustering*).

Au cours des dernières années, les services de renseignement des pays les plus riches ont investi dans les nouvelles technologies, notamment en partenariat avec la Chine et Israël[20]. Bénéficiant traditionnellement d'une place centrale dans l'espace ANMO, les services ont un accès privilégié aux fichiers et bases de données des autres administrations et même du secteur privé[21]. La productivité rendue possible par la technologie leur a permis d'accéder à des volumes de données considérables, disponibles sur une multitude de supports (téléphones, ordinateurs, voitures, biométrie, traces numériques diverses).

Dans presque tous les pays de la région, ils ont accès aux caméras de surveillance déployées par millions dans les villes, ainsi qu'aux données détenues par les opérateurs téléphoniques. Les techniques d'identification des plaques d'immatriculation et de reconnaissance faciale, couplées à de l'IA, se développent dans plusieurs pays (Émirats arabes unis [EAU], Irak, Israël, Qatar). Les plus avancés dans ce domaine sont sans doute les EAU et Israël. Dès 2010, la police de Dubaï avait démontré l'efficacité de son système de caméras de surveillance, lorsqu'elle avait dévoilé une opération du Mossad[22]. Depuis, les EAU ont

20. James Lynch, « Iron Net: Digital Repression in the Middle East and North Africa », Policy Brief, European Council on Foreign Relations, juin 2022.

21. Agnès Levallois, « Les appareils sécuritaires arabes : ultimes remparts de régimes à bout de souffle », *Revue internationale et stratégique*, 121, printemps 2021, p. 97-103.

22. En quelques jours, la police de Dubaï a enquêté sur l'assassinat d'un cadre du Hamas dans un hôtel, en exploitant des quantités de données (caméras de surveillance, données de l'immigration, etc.). Étant arrivée à la conclusion qu'un commando du Mossad avait perpétré l'assassinat, elle a publié les photos des 27 agents israéliens impliqués.

déployé des systèmes de surveillance pour leurs infrastructures critiques (frontières, ports, aéroports, installations pétrolières) mais aussi, de plus en plus largement, dans l'espace public[23]. À Abou Dhabi, le projet *Falcon Eye* combine diverses fonctions de surveillance, de prévention du crime et de gestion des situations d'urgence. L'armée israélienne a déployé des outils de reconnaissance faciale dans 27 points de passage, afin d'identifier les Palestiniens se rendant de Cisjordanie en Israël[24]. En Arabie, la province de La Mecque a déployé un système de surveillance du pèlerinage. Des données sont collectées par des caméras, mais aussi par des bracelets individuels portés par les pèlerins[25].

L'analyse de données est employée de manière croissante comme un outil complémentaire dans les enquêtes criminelles, la lutte contre les trafics et le terrorisme, entre autres. Elle permet, par exemple, de tracer des circuits financiers opaques ou de reconstituer le patrimoine d'un individu qui cherche à le dissimuler.

Divers outils ont été déployés, dont certains ont connu un grand succès : le logiciel Analyst's Notebook, utilisé par la plupart des forces de sécurité de la région ANMO, ou encore Predpol, qui s'appuie sur des cartes représentant la répartition spatiale de la délinquance[26]. Une fois alimentées en données relatives à une enquête particulière (procès-verbaux de plaintes, interrogatoires, expertises), ces applications établissent des liens entre les faits criminels, leurs auteurs et d'autres paramètres qui s'y rapportent (lieux, modes opératoires, etc.). Elles requièrent un surcroît de travail initial dans l'élaboration d'une base de données dans le système d'information, mais au final, elles produisent des résultats auxquels les enquêteurs, pris individuellement, n'auraient

23. Ce programme de surveillance a été confié à trois sociétés par l'Autorité des infrastructures nationales stratégiques.

24. L'entreprise israélienne AnyVision aurait déployé ces dispositifs à partir de 2019 (Marwa Fatafta et Dima Samaro, « Exposed and Exploited: Data Protection in the Middle East and North Africa », Accessnow, janvier 2021).

25. Ce système est exploité par la société Gartner (Steven Feldstein, *The Global Expansion of AI Surveillance*, Carnegie Endowment for International Peace, septembre 2019, p. 16).

26. Développé dans les années 1990 par la société I2 (rachetée depuis par IBM).

pas pu parvenir. Les algorithmes permettent également d'élaborer des analyses prédictives (probabilité de survenue des actes délinquants et criminels). Leur valeur ajoutée repose sur la mise en commun d'une masse de données, qui permet des analyses à grande échelle, génératrices de connexions et de tendances. La puissance de l'IA est censée optimiser les ressources policières.

Palantir est la société de référence dans ce domaine du *law enforcement*, proposant notamment son logiciel Gotham. Enquêtant sur l'assassinat du journaliste américain Daniel Pearl, décapité au Pakistan en janvier 2002, Palantir avait créé une « carte humaine » reliant 27 individus ayant un lien avec ce meurtre[27].

En outre, ces outils d'analyse et d'investigation permettent des synergies dans le cadre des coopérations internationales. Des organisations internationales sont spécialisées dans la mise en commun de données relatives au crime transnational. À elle seule, Interpol gère 18 bases de données (profils ADN, objets et documents volés, trafic d'armes…). D'autres utilisent des outils d'analyse collaborative à des fins de surveillance ou d'enquête. L'UNODC (Office des Nations unies contre les drogues et le crime) développe des programmes de collecte et d'analyse des données sur le trafic d'armes légères et de drogue, notamment pour la région ANMO[28].

Par ailleurs, certaines initiatives d'analyse collaborative viennent de la société civile. Certaines ONG réunissent des données de sources diverses pour lutter contre des réseaux criminels transnationaux, comme cette plateforme en *open data* destinée à combattre les trafics humains dans 150 pays[29].

La collecte, l'analyse et l'exploitation des données pour lutter contre le crime organisé peuvent être catalysées par une approche collaborative. De nombreux sites permettent de

27. https://www.palantir.com/wp-assets/wp-content/uploads/2012/06/ImpactStudy_PearlProject.pdf.

28. https://www.unodc.org/middleeastandnorthafrica/en/overview/overview.html.

29. Counter-Trafficking Data Collaborative (CTDC), https://www.ctdatacollaborative.org/about-us.

recueillir des données publiques (photos, vidéos, enregistrements audio, localisations GPS) pour aider à retrouver des criminels[30]. La police de Dubaï encourage chacun à rapporter des faits délictueux, et même à dénoncer des comportements jugés déviants, *via* l'application Police Eye. C'est sur la base de telles dénonciations qu'en 2020, elle a arrêté une influenceuse qui incitait, sur son compte Instagram, ses *followers* à ne pas respecter les consignes sanitaires[31]. Aujourd'hui, la police de Dubaï utilise les données et l'IA aussi bien pour prévenir la délinquance que pour appréhender les contrevenants. Quelque 10 000 caméras de surveillance sont déployées. Elles seront bientôt reliées à un système de reconnaissance faciale, permettant des contrôles policiers sans contact physique.

Les réseaux sociaux sont de puissants outils collaboratifs, mais ils peuvent être aussi bien utilisés à des fins malveillantes que vertueuses. Le projet ATHAR[32] (The Antiquities Trafficking and Heritage Anthropology Research) s'appuie sur Facebook pour retrouver des antiquités disparues ou volées, précisément parce que les groupes criminels utilisent ce réseau social pour leurs trafics, principalement au Moyen-Orient[33]. Facebook (comme d'autres réseaux sociaux) est également utilisé par la police des Émirats pour faciliter la collecte d'information criminelle par la police[34]. D'autres applications collaboratives s'appuient sur les réseaux sociaux pour combattre les activités criminelles ou condamnables, comme l'abus de mineurs.

30. Postacrime.com, Spotcrime.com, CrimeReports sont populaires aux États-Unis.

31. L'influenceuse (française) se fait appeler The Trendy Frenchie (https://www.instagram.com/the_trendy_frenchie/?hl=fr), https://www.arabnews.com/node/1646536/lifestyle.

32. Projet de The Day After – Heritage Protection Initiative avec l'ACCO, l'alliance pour contrer le crime en ligne.

33. Amr al-Azm, Katie A. Paul, « Facebook's Black Market in Antiquities: Trafficking, Terrorism and War Crimes », ATHAR project, juin 2019 ; et https://atharproject.org/.

34. Awad al-Baloushi, *The effective use of social media in crime detection and prevention: The promotion of public trus in UAE police*, Cardiff Metropolitan University, 2019.

Le ciblage à partir des données est particulièrement utilisé dans le cadre du renseignement financier. Cette mission est exécutée par les États eux-mêmes, au travers d'agences de renseignement financier, agissant au profit de l'exécutif ou de la justice[35]. Néanmoins le secteur privé occupe une part croissante dans l'investigation, notamment pour protéger des entreprises et des particuliers contre les comportements criminels et malveillants, en particulier les actions cyber. Le développement progressif des cryptomonnaies et la digitalisation des relations d'affaires font naître des besoins importants d'information et d'investigation, afin de contrer l'opacité recherchée par certains acteurs.

De nombreuses sociétés (souvent de petite taille) proposent des services d'investigation. Elles utilisent une grande palette d'outils (dont de nombreux à base d'OSINT), afin de vérifier la probité des parties prenantes et le sérieux des transactions.

La donnée ne permet pas seulement de traquer de nouvelles formes de délinquance financière (*via* les cryptoactifs[36]). Elle sert aussi à lutter contre les groupes mafieux et terroristes ayant recours à des montages complexes, afin d'opacifier leurs circuits financiers et de dissimuler leurs avoirs. Certaines associations (y compris françaises), qui camouflent des activités criminelles derrière un paravent caritatif, se financent à partir de fonds provenant du Moyen-Orient et difficiles à tracer[37]. En 2016, une levée de fonds pour des combattants jihadistes a été lancée par l'Ibn Taymiyya Media Centre (campagne Jahezona). Les organisateurs de cette collecte promettaient aux donateurs un complet anonymat, en désignant des adresses bitcoin, *via* l'application

35. Quatorze pays de la région ANMO se sont dotés d'unités spécialisées (unités de renseignement financiers – *financial intelligence units*) pour lutter contre le blanchiment d'argent et le financement du terrorisme (https://www.economie.gouv.fr/particuliers/cryptomonnaies-cryptoactifs#).

36. Les cryptoactifs sont des actifs virtuels stockés sur un support électronique type chaîne de blocs.

37. Tendances et analyse des risques de blanchiment de capitaux et de financement du terrorisme en 2018-19, TRACFIN.

Télégram[38]. En 2019, les brigades al-Qassam ont sollicité des dons en bitcoins par Telegram et Twitter. L'augmentation considérable des transactions en cryptomonnaies dans la région ANMO (dont la composante criminelle ou terroriste ne représente, heureusement, qu'une infime partie) contraint les gouvernements eux-mêmes à recourir aux technologies des données pour tenter de réguler le phénomène[39]. Parallèlement, le réseau TOR[40] est utilisé par la mouvance jihadiste pour dissimuler des pratiques criminelles – davantage pour les transactions financières que pour la propagande ou le recrutement[41].

L'analyse des données est une composante cruciale de la cybersécurité et la cyberdéfense. Cette recherche est définie comme l'analyse de la menace cyber, ou *cyber threat intelligence* (CTI). Selon la définition de l'ANSSI, il s'agit de l'ensemble des activités de recueil, d'étude et de partage d'informations liées à des attaques informatiques[42]. Elle permet d'identifier les menaces émergentes, de capitaliser sur celles passées et mettre en place des systèmes d'alerte. Ces opérations d'investigation s'appuient largement sur l'OSINT, notamment quand il s'agit de rechercher des preuves après une attaque cyber (*forensic digital analysis*).

Enfin, les techniques de ciblage ont été mobilisées de manière accélérée lors de la pandémie de Covid-19. Diverses applications de traçage des citoyens ont été déployées, de manière plus ou moins obligatoire et plus ou moins intrusive. Significativement,

38. Eitan Azani et Nadine Liv, *Jihadists'Use of Virtual Currency*, International Institute for Counter Terrorism, Herzliya, janvier 2018.

39. Sarah Johansson et Mohammed Soliman, « Cryptocurrencies in the Middle East », podcast du Middle East Institute, 2021.

40. The Onion Routing (TOR) est un réseau informatique, développé par un laboratoire de l'US Navy, offrant une certaine anonymisation à ses utilisateurs et permettant d'accéder à certains sites non accessibles sur le web classique. Outre les pays occidentaux, il est fortement utilisé en Israël, en Syrie et en Iran.

41. Miron Lakomy, « Exploring the digital jihadist underground on the Onion Router », *Small Walls Journal*, 30 mai 2021.

42. https://www.ssi.gouv.fr/administration/principales-menaces/analyse-de-la-menace/.

les pays du Golfe et Israël ont adopté des applications parmi les plus intrusives recensées dans le monde[43].

TRACER LES INDIVIDUS

En combinant les techniques d'identification, de classement et de géolocalisation, la donnée permet de discriminer les individus ou les objets en fonction de leurs caractéristiques, de les regrouper (*clustering*) et ainsi de les tracer.

Le domaine de la santé est à la fois prometteur et intrusif. Grâce aux technologies toujours plus sophistiquées, la médecine moderne recourt massivement aux données (biologiques, pathologiques, génétiques, pharmaceutiques, expérimentales). Les données produites par les capteurs corporels connectés, comme celles permises par les progrès de la médecine (génome humain, séquençage ADN) permettront de détecter des pathologies, mais aussi de catégoriser les individus. Des programmes d'identité numérique, de passeports biométriques et de services médicaux en ligne ont été développés dans de nombreux pays de la zone ANMO.

La crise sanitaire de Covid-19 a fourni un excellent terrain d'expérimentation aux dispositifs de traçage des individus ou de contrôle des confinements. Israël a adopté un dispositif pour détecter et localiser les possibles contaminations à la Covid-19. Ce système s'est appuyé sur l'expertise du renseignement intérieur (Shin Bet), à partir de la localisation des téléphones mobiles[44]. La Tunisie a mis en place un système de localisation par les cartes SIM, mais aussi des robots équipés de caméras infrarouges pour vérifier l'application des mesures de distanciation[45].

43. Voir dans la deuxième partie, la section « Une exposition forte à la surveillance numérique ».

44. D'autres pays dans le monde ont eu recours à des technologies similaires (Chine, Corée, Russie, Suisse).

45. Page Facebook du ministère de l'Intérieur tunisien : https://www.facebook.com/ministere.interieur.tunisie/videos/1106579619691659/?v=1106579619691659.

Les possibilités de traçage et de discrimination ne se limitent pas au seul domaine médical. Les autorités recourent à ces technologies pour identifier et tracer un individu avec un grand niveau de fiabilité. Les applications sont évidentes dans le domaine de l'état civil et de l'administration. Ainsi, les pays du Golfe mettent en place des cartes d'identité numériques et des applications associées. La biométrie permet de répertorier des individus qui ne sont pas enregistrés dans les bases de données ou qui n'ont pas d'adresse fixe. Elle permet aussi aux autorités d'enregistrer les données corporelles (visage, iris, empreintes digitales) des personnes qui entrent sur le territoire, comme le font, entre autres, Israël et la Jordanie[46].

Le traçage ne vient pas seulement de décisions gouvernementales. Dans bien des cas, ce sont surtout les individus eux-mêmes qui produisent des traces numériques, au travers de leurs activités en ligne (moteurs de recherche, réseaux sociaux, commerce électronique, téléphone, transport). Ces traces permettent de répartir les individus en fonction de leurs opinions, de leurs profils de consommation ou autres critères, pour mener des approches ciblées.

*

Au regard des quatre éléments envisagés, les nouveaux usages permis par l'utilisation des données concourent à l'évidence à une meilleure compréhension des situations et des phénomènes, en région ANMO (comme ailleurs). Ceux qui veulent acquérir, stocker ou analyser l'information disposent d'outils technologiques d'une puissance inédite, capables à la fois de collecter des données facilement (à distance, depuis le ciel) et d'accroître la précision et la qualité de l'information détenue. Cette information acquiert une valeur encore plus grande si elle est traitée et analysée, au moyen de l'intelligence artificielle ou humaine.

46. En croisant les données biométriques capturées sur l'individu et celles scannées sur le passeport, les polices des frontières compliquent le déplacement des faux profils (malfaiteurs et espions).

En outre, la donnée ne permet pas seulement de savoir et de comprendre mais aussi de prévoir, à partir de modèles mathématiques et de corrélations statistiques. Le *big data* n'explique pas toujours pourquoi un phénomène va se produire, mais il peut anticiper son occurrence avec une forte probabilité. Cette capacité est utilisée dans l'industrie, l'énergie, la finance, le marketing, le transport, le pilotage de projets ou la santé. L'espace ANMO est engagé dans ce processus, au même titre que les autres régions du monde les plus connectées.

La connaissance procurée par la donnée multiplie les possibilités offertes pour agir sur l'environnement : piloter, surveiller, investir, communiquer, contrôler[47]. Naturellement, la qualité de la connaissance dépend de la quantité et de la valeur des données recueillies. À cet égard, il convient de s'interroger sur le degré d'exposition qu'offre la région ANMO au recueil de ces données.

47. On citera par exemple la gestion des villes connectées et le pilotage de projets d'infrastructure qui s'appuient sur l'analyse des données collectées en temps réel.

II. NUMÉRISER LA RÉGION ANMO

Une donnée ne peut être collectée et analysée que si le réel a été préalablement « numérisé » : cette numérisation s'apparente à un codage des informations, afin que celles-ci puissent être – une fois collectées – mémorisées par un système informatique, puis rapprochées avec d'autres informations du même type. Or la région ANMO présente une exposition contrastée à cette numérisation. D'un côté, l'accès aux données fait l'objet d'un contrôle gouvernemental souvent restrictif ; de l'autre, à l'inverse, le manque de régulation et l'insuffisante protection des données personnelles laissent plus d'espace à la surveillance et aux technologies de collecte.

LES BARRIÈRES AU TRAVAIL D'INVESTIGATION

Le travail de journaliste ou de chercheur y est plus compliqué que dans d'autres régions du monde pour au moins deux raisons : le manque de ressources disponibles et le contrôle socio-politique. En outre, le recueil d'information peut être compliqué par les déterminants culturels.

Des codes difficiles à déchiffrer sans une fine compréhension culturelle

Un chercheur étranger à la région ANMO peut difficilement s'appuyer sur des agrégats de données pour appréhender des situations complexes ou, tout simplement, pour percevoir les tendances de l'opinion. C'est son expérience qui lui permet d'orienter sa recherche d'informations (y compris en données quantitatives) mais aussi d'invalider des hypothèses résultant pourtant de l'analyse de données.

Plusieurs années après un travail de recherche sur les opérations militaires émiriennes au Yémen, Pierre-Jacques Teisseire estime que la collecte d'informations ouvertes l'aurait conduit

sur de fausses pistes, s'il n'avait pas pu s'appuyer sur une solide expérience personnelle. Pour lui, le développement de la connaissance par les données ne permettra pas de remplacer le « flair, acquis par une longue acculturation académique, des expériences de terrain et la fréquentation prolongée des populations locales ». La notion d'intelligence culturelle, utilisée par les militaires et les services de renseignement, fait référence à une appréhension « à large spectre » du théâtre d'opérations.

Une production de données inégale

Le niveau d'intérêt pour la région ANMO ne se traduit pas forcément en termes de données à collecter.

Les pays ravagés par la guerre et les crises (Irak, Liban, Libye, Syrie et Yémen) et les pays très pauvres ne parviennent pas à réaliser des enquêtes ni à publier des statistiques de manière stable. Dans les régions désertiques et enclavées, l'absence de couverture internet limite évidemment la production de données. Quand l'UNODC établit un bilan des saisies de cannabis en Afrique du Nord, il doit s'en remettre au bon vouloir des États membres. La carte qui en résulte révèle d'importantes zones grises.

La région connaît de très grandes disparités en matière de recherche et de publications scientifiques. Plusieurs pays (Qatar, Arabie, Tunisie) sont très prolifiques (plus de 200 publications par million d'habitants) tandis que les derniers du classement ne produisent presque rien[1].

Un manque de ressources disponibles en ligne

Les ressources officielles (dans le domaine administratif ou commercial), permettant de recueillir de l'information de source première, sont très inégales. Dans plusieurs pays, les informations administratives et légales sont difficilement accessibles. D'après un avocat exerçant dans la région depuis longtemps,

1. Rapport de l'UNESCO sur la science, 2014, https://fr.unesco.org/Rapport_UNESCO_science/etats_arabes.

cette disparité est voulue par les élites locales afin de privilégier les familles bien implantées (*insiders*), au détriment des avocats et des hommes d'affaires extérieurs au pays (*outsiders*)[2]. On trouve bien des journaux officiels dans plusieurs pays d'ANMO[3], mais leur contenu est en général restreint.

L'information de nature économique est également difficilement accessible. Les législations nationales imposent rarement aux sociétés de publier leurs comptes annuels et leurs opérations financières dans un bulletin d'annonces obligatoires. De ce fait, les cabinets de conseil établis en Europe et en Amérique du Nord ont du mal à obtenir les informations dont ils ont besoin. Ces données sont parfois publiées dans des revues spécialisées, mais d'une manière aléatoire et changeante, comme pour brouiller les pistes[4]. Dans les pays du Golfe, le travail d'enquête est rendu d'autant plus compliqué que les dirigeants d'entreprises, tout comme les gestionnaires de patrimoines, recherchent généralement le secret des affaires. Le recours à des montages financiers complexes (cascade de holdings, notamment dans des paradis fiscaux) sert d'écran protecteur. L'accès aux données est alors impossible par moyens ouverts, sauf à identifier des failles dans la dissimulation. Par exemple, on peut tracer les flux financiers lorsqu'ils quittent les paradis fiscaux pour être réinvestis dans l'économie légale. C'est ce que s'emploient à faire certains cabinets d'investigation.

L'investigateur peut mettre à profit certaines particularités régionales des pays du Golfe. Dans le domaine du droit commercial, par exemple, les partenariats entre sociétés locales et étrangères doivent faire l'objet d'un enregistrement et d'une publicité[5]. La structure tribale de la société fournit aussi des

2. Entretien avec un avocat exerçant dans la région du Golfe depuis les années 1990.

3. Algérie, Arabie, Égypte, EAU, Iran, Israël, Koweït, Maroc, Oman, Palestine, Qatar, Tunisie ont des annonces légales publiques accessibles sur internet (gazettes).

4. Entretien avec Joël Rey, associé gérant de la société ASTARTE.

5. Au Koweït, ces accords de représentation sont déposés à la Chambre de commerce. Un enquêteur (ou un concurrent) peut donc connaître les

angles d'attaque intéressants pour le travail d'enquête. L'étude des noms de famille étendus, qui comprennent les patronymes des ascendants, permet de reconstituer des filiations généalogiques et, ainsi, les liens familiaux entre des individus[6].

Dans certains cas, l'accès aux informations légales nécessite un travail de démarchage, qui ne peut se faire à distance et qui exige l'accès aux bonnes personnes (greffes des tribunaux, par exemple). Même en démarchant, l'obtention d'un document peut réclamer du temps. Ce délai peut être mis à profit par celui qui détient une information exclusive, avant qu'elle ne soit partagée[7]. Les citoyens eux-mêmes n'ont pas d'accès garanti à leurs propres données personnelles. En cas de procédure judiciaire ou administrative, ils peuvent se voir opposer un refus d'accès par l'administration compétente ou le tribunal en charge de l'affaire[8].

Toutefois, une tendance à la transparence est nettement engagée dans la région ANMO. De nombreux États ont entrepris de véritables efforts pour digitaliser leur administration. Les pays du Golfe ont inscrit cet engagement dans le cadre de leurs stratégies nationales *(Saudi Vision 2030, Egypt Vision 2030, Qatar Vision 2030, Kuwait Vision 2035, Oman Vision 2040*, etc.). La crise sanitaire a accéléré la prise de conscience et les démarches engagées. Dans certains cas, les résultats sont spectaculaires : Oman et les EAU occupent respectivement la 11e et la 17e place du classement ODIN, qui prend en compte le volume de données disponibles et le niveau de transparence[9]. Aux Émirats, le portail de données ouvertes donne non seulement accès à des dizaines d'administrations en ligne, mais il procure également de très nombreuses statistiques utiles aux journalistes et aux chercheurs[10]. Le portail qatarien Hukoomi rassemble 293 entités accessibles en ligne[11].

partenariats établis par une société donnée. En revanche, les transactions ne sont pas déclarées.

6. Entretien avec Joël Rey.
7. Entretien avec Alexis Vinette, consultant dans le cabinet FTI.
8. Entretien avec un cadre d'une société de renseignement d'affaires.
9. Open Data Inventory, https://odin.opendatawatch.com/.
10. http://data.bayanat.ae/en_GB/dataset.
11. https://hukoomi.gov.qa/en/.

Si, au Koweït, la digitalisation administrative progresse malgré d'importantes disparités[12], elle a été faiblement engagée en Algérie (163e du classement ODIN), en Syrie (167e) et en Libye (181e).

Un contrôle politique et social souvent étroit

Les sociétés de la région ANMO font l'objet d'un contrôle politique et social traditionnellement étroit. Parmi les explications possibles de cette singularité moyen-orientale, on citera celle avancée par le grand historien du monde arabe Ibn Khaldoun. Pour lui, le pouvoir n'est pas fondé sur la cité, comme dans la tradition grecque, mais sur le regroupement (*'asabiya*) et sur « un lien du sang tribal et familial ». Cette *'asabiya* « acquiert une force sans commune mesure quand elle parvient à prendre le contrôle de l'appareil d'État », au travers des familles des dirigeants qui dominent les ministères clés, et notamment les services de renseignement[13]. Ce contrôle politique constitue à l'évidence une barrière au travail d'investigation. Les lignes rouges tracées par le pouvoir sont très respectées dans les monarchies, un peu moins dans les républiques. À titre d'exemple, les sondages politiques sont interdits dans les pays du Golfe, et cette consigne est respectée.

Dans la région ANMO, on observe une grande diversité de régimes politiques qui vont de la monarchie à la république islamiste en passant par des républiques parlementaires tendant à l'autoritarisme, le tout avec une certaine propension aux coups d'État. La plupart d'entre eux affichent un rejet du modèle occidental, la démocratie libérale. En effet, contrairement à la tendance mondiale à la démocratisation, certains États du Maghreb

12. Le ministère de l'Intérieur progresse rapidement vers le e-gouvernement (documents d'identité, résidence et permis de conduire en ligne, par exemple) alors que d'autres administrations marquent le pas. La Central Agency for Information Technology peine à coordonner les initiatives.
13. Philippe Droz-Vincent, « Quel avenir pour l'autoritarisme dans le monde arabe », *Revue française de science politique*, 54:6, 2004, p. 945-979.

et du Moyen-Orient n'ont pas tenté l'expérience démocratique ou du moins elle n'a pas duré.

Plusieurs de ces régimes cadenassent la société afin d'asseoir leur pouvoir. Outre une mainmise forte sur la politique, ils exercent un véritable contrôle de l'information.

Par ailleurs, les informations touchant à la sécurité sont très soigneusement protégées. Les services de sécurité (forces armées, police, services de renseignement) diffusent peu d'informations par l'intermédiaire des sites web et de la presse. Ils inculquent à leurs cadres une culture du secret suffisamment efficace pour générer de l'opacité. Même des informations apparemment anodines, comme des opérations de relations publiques, ne peuvent être photographiées sans autorisation[14]. Les législations nationales restreignent souvent l'expression des internautes sur la toile, au nom de la sécurité nationale. En Jordanie, on peut être poursuivi pour avoir critiqué les monarchies du Golfe sur les réseaux sociaux[15]. Aux EAU, les appels téléphoniques en VoIP sont bloqués par les autorités depuis janvier 2018[16]. Cette interdiction a d'ailleurs été particulièrement critiquée pendant la crise sanitaire, en raison des besoins en communication à distance dans le domaine professionnel et pour l'enseignement. Ce blocage des réseaux sociaux et des messageries instantanées est également pratiqué par l'Iran[17], ainsi que, de manière occasionnelle, par l'Irak et d'autres pays. Au Liban, le Hezbollah a une

14. Dans la plupart des armées arabes, il existe une direction de l'orientation morale (*morale guidance*) qui doit donner son autorisation pour que se tienne la moindre opération de relations publiques.

15. La loi 55 portant sur la lutte contre le terrorisme (adoptée en 2006, amendée en 2014) interdit de publier des contenus « perturbant les relations avec un État étranger ».

16. Les solutions de communication « Voix sur IP » (Skype, Whatsapp, etc.) ont été interdites aux EAU.

17. Facebook, Twitter, Telegram et YouTube sont bloqués. Toutefois beaucoup d'Iraniens parviennent à utiliser ces applications au moyen d'un VPN.

stratégie de sanctuarisation, qui se décline aussi dans l'espace numérique (contrôle de la production de données)[18].

Les journalistes sont très contrôlés. Ceux qui travaillent dans de grands médias sont soumis à une discipline de rédaction assez stricte. Les indépendants sont également contrôlés par l'État. De ce fait, le journalisme indépendant est moins développé qu'en Occident. Sans surprise, ce contrôle de l'information par l'État est particulièrement prégnant dans les régimes autoritaires. L'ONG Reporters sans frontières (RSF) établit annuellement un classement sur la liberté de la presse, dans lequel les pays du Moyen-Orient occupent les dernières places : l'Arabie saoudite (172e en 2019), la Syrie (174e) et l'Iran (170e) figurent parmi les dix pays en queue de classement. Selon RSF, les journalistes s'exposent aux violences physiques ou à la prison « quand ils ne se conforment pas aux injonctions au silence ou à la propagande étatique[19] ». La crise sanitaire a été l'occasion pour certains gouvernements d'adopter des législations destinées à « lutter contre les fausses informations », ou à affaiblir les possibilités de mobilisation[20]. Certains États refusent d'accorder des visas à des journalistes ou à des chercheurs désireux de venir enquêter dans le pays[21]. Ce contrôle de l'information, associé à l'essor des réseaux sociaux, a tendance à détourner la population des médias traditionnels. Au Qatar, la confiance du public vis-à-vis des médias traditionnels a chuté de 12 points entre 2017 et 2019[22]. D'après RSF, la liberté de

18. Olivier Passot, « La stratégie d'Israël face au renforcement du Hezbollah – La centralité du renseignement », Note de recherche 87, IRSEM, 28 janvier 2020, p. 6.

19. https://rsf.org/fr/actualites/classement-mondial-de-la-liberte-de-la-presse-2019-les-analyses-regionales.

20. https://rsf.org/fr/classement-mondial-de-la-liberte-de-la-presse-2020-nous-entrons-dans-une-decennie-decisive-pour-le.

21. https://mesana.org/advocacy/committee-on-academic-freedom/2017/01/04/blacklisting-and-harassment-of-scholars.

22. Ce niveau de confiance est passé de 69 % à 57 % de 2017 à 2019, une tendance observée également en Arabie et en Tunisie (« Media use in the Middle East, a Seven-Nation Survey », Northwestern University in Qatar, 2019, http://www.mideastmedia.org/survey/2019/uploads/file/NUQ_Media_Use_2019_WebVersion_FNL_051219%5B2%5D(1).pdf).

la presse progresse toutefois en Afrique du Nord, notamment en Tunisie (72e de ce classement).

Cette difficulté des journalistes à exercer leur activité en incite certains à s'installer à l'étranger. Toutefois, la distance rend souvent leurs analyses moins pertinentes et leurs investigations moins rapides.

L'important contrôle politique et social génère par ailleurs certains biais cognitifs. Les médias s'interdisent de traiter certains sujets polémiques ou d'exprimer des critiques à l'encontre du pouvoir. Dans les pays du Golfe, les journalistes questionnent rarement les politiques publiques. Cette autocensure peut s'expliquer par la proximité entre le pouvoir et les organes de presse. Dans les pays du Golfe, les fonctions de direction des grandes entreprises privées (y compris les médias et les sociétés de communication) sont souvent occupées par des membres des familles royales et princières. En Irak, il existe une véritable diversité des médias, mais elle est sous-tendue par des rivalités politiques et confessionnelles : les journaux et chaînes télévisées sont liées à des partis, qui ont tendance à diffuser « la voix de leur maître » plutôt qu'une information libre et pluraliste[23]. Sans se limiter à un pays, l'UNESCO relève une « communautarisation croissante des médias », qui a tendance à produire des biais culturels ou religieux dans le traitement de l'information[24].

Par ailleurs, les rivalités politiques et communautaires, qui traversent plusieurs pays de la zone, engendrent d'autres biais cognitifs (théories du complot, diabolisation du camp antagoniste)[25]. Cette polarisation de l'opinion est renforcée par le recours parfois exclusif aux réseaux sociaux comme source d'information. Elle expose les individus au risque de manipulation (voir paragraphe suivant).

23. Gilles Chenève, *Panorama de l'Irak contemporain*, Paris, Éd. du Cygne, 2017, p. 75. Selon lui, la profusion de médias est un trompe-l'œil qui cache des affiliations systématiques à des partis ou à des hommes d'affaires.

24. United Nations Educational, Scientific, and Cultural Organization, World Trends in Freedom of Expression and Media Development: Regional Overview of Arab States 2017/2018, Paris, UNESCO, 2018.

25. Entretien avec Alexis Vinette, consultant chez FTI.

Une part imprévisible malgré les données et leur analyse

La concentration du pouvoir, évoquée précédemment, vaut aussi pour les ressources informationnelles. Dans des systèmes politiques très centralisés, comme il en existe en région ANMO, la connaissance est concentrée dans les mains d'un petit nombre de personnes, voire d'une seule. Dans un modèle politique où le processus décisionnel est totalement cloisonné, la collecte automatisée de données est inopérante. Si les algorithmes avaient existé en 1990, auraient-ils pu prévoir que Saddam Hussein allait décider d'envahir le Koweït ? Selon de nombreux experts, le président irakien a pris seul cette décision. Pouvoir prédire une telle décision semble d'autant plus illusoire si l'on admet que Saddam s'est fié davantage à son instinct qu'à des critères rationnels[26]. En revanche, des événements rendus possibles par des rassemblements de masse ou par l'agrégation d'opinions favorables sont susceptibles d'être anticipés à partir des données. Ainsi, plusieurs chercheurs ont estimé que les révoltes arabes de 2011 étaient prévisibles, à partir des revendications à caractère économique, social et politique[27].

Les technologies prédictives sont réputées efficaces pour anticiper des phénomènes récurrents ou « prévisibles », à partir de modèles qui ont été établis au préalable. Cependant, par définition, elles ne permettent pas de détecter des événements inédits ou qui ne reposent pas sur des données quantitatives. Or, la région ANMO est fertile en évolutions brutales et en surprises stratégiques. Le chercheur Ephraïm Kam estime que le Moyen-Orient connaît des évolutions rapides et peu prévisibles, en raison des montées de violence régulières et du manque de stabilité des régimes[28]. Précisément, les phénomènes de violence poli-

26. Alice Miller, « When Saddam Hussein Invaded Kuwait », The Mindbody Spot, 1997.

27. Simplice A. Asongu, Jacinta C. Nwachukwu, « Revolution Empirics: predicting the Arab Spring », *Empirical Economics, Journal of the Institute for Advanced Studies*, Vienne, 29 octobre 2015.

28. Il prend pour exemples la guerre des Six-Jours, la chute du shah d'Iran, le déclenchement de la guerre du Liban de 2006 et la série des Printemps arabes

tique ont tendance à créer de l'incertitude dans divers domaines de la vie économique et sociale. D'après un expert financier du Moyen-Orient, les données sont peu pertinentes pour anticiper les événements géopolitiques et l'évolution du prix du baril de pétrole. Or, « ce sont deux paramètres qui influencent tous les autres, et qui sont eux-mêmes corrélés[29] ».

Une insécurité préjudiciable au journalisme de terrain

Dans les zones de guerre et de crise, l'insécurité constitue un obstacle au travail d'investigation journalistique. Les reporters s'exposent à la fois au danger des affrontements, au risque physique d'être pris à partie par un belligérant, ainsi qu'à celui de finir en prison. Dans des conflits aux fronts lacunaires, comme en Syrie, ils peuvent passer d'une zone contrôlée par un groupe armé à une autre en l'espace de quelques kilomètres, risquant sans cesse d'être pris en otages.

A contrario, ces barrières à l'investigation confèrent un intérêt particulier aux méthodes d'investigation fondées sur la technologie. Pour mener une enquête dans une zone de guerre, il est bien plus commode d'organiser une campagne de collecte et d'analyse de données à distance, que d'envoyer des enquêteurs ou des journalistes sur le terrain[30]. Les risques qui pèsent sur le patrimoine architectural de la région ANMO poussent d'ailleurs certains acteurs à le numériser grâce aux technologies récentes, à défaut de pouvoir le préserver. Plusieurs sociétés se sont spécialisées dans la modélisation des sites en péril ou partiellement détruits par la guerre, comme Alep, Palmyre ou encore Tombouctou[31].

(Ephraim Kam, « The Middle East as an Intelligence Challenge », *Strategic Assessment*, 16:4, janvier 2014).

29. Entretien avec le responsable d'une grande banque établie dans le Golfe.

30. Entretien avec Emmanuel de Dinechin (président de MASAE), 11 septembre 2020.

31. Iconem utilise des drones pour scanner les sites sous tous les angles afin de les modéliser en 3D, https://iconem.com/fr/.

Reconstitution en 3D du site syrien de Palmyre (exposition *Sites éternels – de Bâmiyân à Palmyre*, Grand Palais, Paris, 14 décembre 2016 – 9 janvier 2017)

La pandémie n'a fait qu'accentuer cette tendance, en empêchant les journalistes de se déplacer dans les zones de conflit et en restreignant les interactions sociales. De plus, elle a conduit les gouvernements à davantage contrôler l'information[32].

Or, les révolutions arabes ont révélé la puissance des médias, qui ont bien souvent joué le rôle d'opposition institutionnelle. Surtout, les réseaux sociaux ont catalysé les mobilisations populaires.

UNE EXPOSITION FORTE DES CITOYENS À LA SURVEILLANCE NUMÉRIQUE

Les individus vivant dans la région ANMO semblent de plus en plus exposés à la surveillance et à la manipulation. Les activités numériques se développent à grande vitesse sans que la question des données personnelles soit particulièrement prise en compte.

32. Index de la liberté de la presse 2020, compilé par Reporters sans frontières, https://rsf.org/en/2020-world-press-freedom-index-entering-decisive-decade-journalism-exacerbated-coronavirus.

Le taux de pénétration digitale est particulièrement élevé chez les jeunes (18-24 ans) de la région ANMO. Neuf jeunes sur dix utilisent au moins un média social quotidiennement (cette proportion monte à 99 % aux EAU)[33]. Plus de la moitié des jeunes s'informent *via* les réseaux sociaux plutôt que par les médias traditionnels (34 % par la télévision et 4 % par les journaux)[34]. Les comportements se digitalisent dans tous les domaines : commerce, banque, transports, rencontres, etc. Ce sont 75 % des jeunes qui ont fait des achats en ligne en 2021, une tendance qui se renforce d'année en année[35]. Derrière ce chiffre se dissimule des disparités importantes liées aux infrastructures, au type de couverture (4G ou 5G), mais aussi à la confiance dans le digital. Quand 90 % des Émiriens effectuent des achats en ligne, c'est le cas d'à peine 10 % des Algériens[36]. Le nombre de comptes Facebook a triplé au cours des dernières années[37]. En Arabie saoudite, Twitter est utilisé activement par 10 millions de personnes (38 % de la population)[38]. Le pays est le sixième marché mondial pour la compagnie américaine. L'expansion de ces plateformes incite les individus eux-mêmes à mettre en ligne leurs données personnelles, ce qui provoque assez de résistances. « Les consommateurs du Moyen-Orient n'hésitent pas à fournir aux sociétés de commerce en ligne des copies de leurs documents administratifs (passeports ou autres) », explique un responsable d'une société technologique.

33. Damian Radcliffe, Hadil Abuhmaid, *Social Media in the Middle East: 2019 in review*, University of Oregon, janvier 2020.

34. Arab Youth Survey 2019, p. 7.

35. Arab Youth Survey 2021 : ce chiffre est passé de 53 % à 71 % de 2018 à 2019. Il est vraisemblablement bien plus élevé depuis la crise de la Covid.

36. Chikhi Kamel, « Le comportement des consommateurs face au e-commerce en Algérie », *Revue internationale du marketing et management stratégique*, 2:3, juillet-septembre 2020.

37. Le nombre de comptes est passé de 56 à 164 millions de 2014 à 2019 (Damian Radcliffe et Payton Bruni, « Social media in the Middle East: five trends journalists need to know about », journalism.co.uk, 15 avril 2019).

38. Damian Radcliffe, « How Twitter Usage in the Middle East is evolving », 26 mars 2020, https://medium.com/@damianradcliffe/how-twitter-usage-in-the-middle-east-is-evolving-deb675089375.

Cette digitalisation croissante des comportements est rendue possible par des investissements considérables dans les infrastructures de communication. La plupart des pays du Golfe se dotent de la technologie 5G (Arabie, Bahreïn, Émirats, Koweït, Qatar), grâce à des infrastructures adaptées (fibre optique, antennes, plateformes), souvent produites et déployées par l'entreprise chinoise Huawei[39]. Cette accélération croissante du débit va, à son tour, augmenter de manière considérable la production de données, confortant ainsi les immenses perspectives offertes par le *big data*.

Or, le numérique est encore assez peu régulé dans la région ANMO. Les gouvernements sont assez complaisants quant au déploiement de nouveaux logiciels (par des acteurs publics ou privés), pour toutes sortes d'usages. Quant aux administrations spécialisées (services de renseignement, police, armée), demandeuses d'outils dédiés (logiciels de surveillance ou d'investigation), c'est encore plus simple : ce sont souvent elles qui délivrent les autorisations. L'utilisateur et l'autorité de régulation se trouvent alors être la même entité[40]. En Israël, l'opinion publique accepte assez facilement des atteintes aux libertés individuelles, quand elles apparaissent justifiées par la lutte contre le terrorisme ou par la santé publique. Cette approche prévaut aussi dans l'ordre international, lorsque les Israéliens font valoir que les intérêts de sécurité sont supérieurs au droit humanitaire[41].

L'Arabie saoudite (ainsi que d'autres pays ANMO) a adopté depuis 2008 une carte d'identité numérique qui contient des informations très personnelles (état civil, données biométriques, adresse, téléphone) pouvant être croisées avec des informations

39. John Calabrese, « The Huawei Wars and 5G Revolution in the Gulf », Middle East Institute, 30 juin 2019.

40. Entretien avec un industriel spécialiste des technologies numériques basé au Moyen-Orient.

41. Nations unies, « Israël : le Comité des droits de l'homme s'interroge sur l'application du Pacte sur les droits civils et politiques dans le Territoire palestinien occupé », 23 mars 2022.

bancaires[42]. Avec la crise sanitaire, le numérique a pénétré encore plus profondément dans la vie quotidienne et dans l'administration, sans que la régulation ait suivi. Des contrats publics ont été attribués aux grandes sociétés technologiques (souvent auprès des ministères de la Santé et de l'Intérieur) pour faire face aux besoins urgents liés à la pandémie. Enfin, dans les zones frappées par les guerres et les crises, les autorités locales parent au plus pressé pour recenser et administrer les populations qu'elles ont sous leur responsabilité. Les Forces démocratiques syriennes ne s'embarrassent pas avec les règles de vie privée pour enregistrer dans leurs bases de données les prisonniers de l'État islamique et leurs familles[43].

Enrôlement par prise d'empreinte digitale d'une détenue du camp d'al-Hol[44]

En Israël, le gouvernement a confié à son service de renseignement intérieur la responsabilité du traçage des individus, pour lutter contre la pandémie de Covid-19. Le Shin Bet a utilisé un système de localisation GPS, les données des opérateurs

42. La société Thales détaille toutes les données contenues dans cette carte d'identité : https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/customer-cases/saudi-arabia.

43. Entretien avec un humanitaire ayant travaillé en Syrie.

44. Source : compte twitter Coordination and Military Ops Center-SDF (https://twitter.com/cmoc_sdf).

téléphoniques et une base de données spécifique au renseignement intérieur (et inconnue du public)[45].

Le développement de la digitalisation n'a pas seulement fourni aux gouvernements des capacités de surveillance accrues. Il a offert d'immenses possibilités à l'investigation privée, même dans des domaines sensibles. Dès 2015, le colonel Pierre-Jacques Teisseire avait pu enquêter sur les opérations militaires conduites par les Émirats arabes unis au Yémen, un sujet pourtant couvert par le secret. Voulant documenter un tir de missile balistique ayant frappé une base militaire au Yémen, il avait pu déterminer le nombre de victimes et même leur origine géographique. Cette recherche avait été possible en consultant les journaux locaux émiriens en ligne, qui publiaient des annonces pour chacune des cérémonies funéraires[46]. Au Koweït, il est aujourd'hui facile de trouver les photos de tous les responsables politiques, économiques et militaires, car ils sont tous présents sur les réseaux sociaux, ce qui était simplement impensable dix ans plus tôt. Enfin, la digitalisation tous azimuts, y compris sa composante biométrique, expose au risque de dissémination des données sensibles à des tiers, potentiellement malveillants. En prenant le pouvoir à Kaboul en août 2021, les Talibans ont récupéré un énorme patrimoine numérique, dont celui accumulé par les forces de la coalition pendant des années. Ils peuvent utiliser ces bases biométriques dans un but totalement différent (représailles contre les « collaborateurs ») de celui prévu par ses concepteurs.

Cette production de données tous azimuts offre des opportunités inédites aux gouvernements ANMO pour exercer les missions régaliennes que sont la sécurité et la justice. À l'inverse, elle les place dans une situation très délicate au regard de la confidentialité de certaines de leurs activités sensibles. Cette tension peut être observée à peu près partout où la donnée est produite.

45. Tehilla Schwartz Altshuler et Rachel Aridor Hershkowitz, « How Israel's COVID-19 mass surveillance works », Brookings, 6 juillet 2020.

46. Entretien avec Pierre-Jacques Teisseire, ancien militaire et chercheur. « Les contre-performances des armées du Golfe au Yémen », *Orient XXI*, mai 2016.

Les Forces de défense israéliennes (FDI) ont déployé une application (*al-Munasiq*) destinée aux Palestiniens qui franchissent régulièrement la barrière de sécurité pour se rendre en Israël. Les utilisateurs de l'application doivent consentir à l'administration israélienne le libre accès à leurs données de localisation, messages, fichiers stockés sur le téléphone, etc.[47]. Pendant la pandémie, les Palestiniens travaillant en Israël n'avaient pas d'autres options que de télécharger cette application, car les bureaux compétents étaient fermés. « Les Israéliens n'ont même plus besoin d'exercer des pressions sur nous pour que nous parlions », confie un Palestinien, conscient des possibilités offertes par la technologie[48]. D'un autre côté, ces mêmes FDI semblent incapables d'empêcher leurs soldats de diffuser des informations *via* leurs téléphones mobiles, lorsqu'ils sont déployés en opérations (ou juste après, si les téléphones sont momentanément confisqués). Le téléphone mobile est également employé massivement dans les armées arabes, y compris dans des configurations opérationnelles (la plupart des belligérants en Irak et en Syrie).

Toutefois les armées de la région ANMO ne sont pas les seules à produire des traces numériques indésirables : de nombreux opérateurs de forces spéciales occidentales, déployées en Irak et en Syrie, se sont fait épingler par la presse car leurs parcours d'entraînement à la course étaient localisables *via* le logiciel Strava[49]. Dans un monde ultra-connecté, il est particulièrement difficile de supprimer l'exposition numérique indésirable, sauf à mettre en place des politiques drastiques vis-à-vis d'internet et des télécommunications, peu soutenables dans la durée. Lorsque l'État islamique contrôlait des régions entières, en Irak et en Syrie, il

47. Entretien avec un Palestinien. Cette application al-Munasiq (« le coordinateur ») est administrée par le COGAT, administration israélienne de coordination des activités gouvernementales dans les territoires.

48. Entretien avec un habitant de Naplouse.

49. Sébastien Sebt, « Strava, l'appli pour coureurs qui en dit long sur les bases militaires secrètes », France 24, 29 janvier 2018.

ne parvenait à imposer le black-out à la population qu'au prix d'une répression féroce[50].

BILAN : UNE RÉGION QUI NE SE LAISSE PAS NUMÉRISER FACILEMENT

La digitalisation croissante de la région ANMO et la relative faiblesse de la régulation plaident en apparence pour une exposition forte à la collecte des données. La technologie facilite l'accès à l'information, ce qui vaut aussi bien pour les gouvernements (missions régaliennes) que pour les acteurs privés. Cette technologie permet en outre de s'affranchir de nombreuses contingences matérielles, comme l'insécurité, l'accès au terrain ou la culture du secret.

La centralisation et la verticalité du pouvoir rendent l'accès aux informations, et surtout à l'analyse, très hasardeuses. Citons encore la décision d'envahir le Koweït (août 1990), mais aussi celle d'Ariel Sharon de retirer les colonies juives de la bande de Gaza (mai 2004) : prises par un seul homme, elles n'auraient sans doute pas été prévisibles par un algorithme. À l'opposé, la technologie peut se révéler utile pour détecter des mouvements d'opinion et anticiper des manifestations à partir des diffusions massives sur les réseaux sociaux, sur le modèle des révolutions arabes.

50. COL Olivier Passot, *L'Activité de renseignement des groupes jihadistes*, Étude 60, IRSEM, novembre 2018, p. 72.

III. QUI SONT LES ACTEURS DE LA CONNAISSANCE PAR LA DONNÉE ?

Un nombre croissant d'acteurs publics et privés recueillent et analysent des données numériques pour améliorer leur compréhension de leurs champs d'action respectifs.

Les acteurs traditionnels de la connaissance stratégique (journalistes, services de renseignement, chercheurs) se trouvent ainsi concurrencés par de nouveaux entrants, que les nouvelles technologies dotent de capacités inédites à produire de l'information.

En référence au cadre de l'étude défini en introduction, on ne s'intéressera ici qu'aux acteurs qui opèrent dans le domaine des informations stratégiques. On exclura par exemple les banques, malgré leurs investissements considérables dans l'analyse des données pour connaître toujours plus précisément leurs clients.

SERVICES ÉTATIQUES

Plusieurs États de la région ANMO ont développé des capacités d'analyse de données, qui sont utilisées entre autres pour la surveillance, la sécurité, le cyber, le respect des normes sanitaires, et certains autres usages développés dans la première partie.

Les services de renseignement recourent volontiers à la surveillance d'internet et des réseaux sociaux, pour lutter contre le terrorisme et pour surveiller les menaces subversives. Cette surveillance est de plus en plus connue par les populations elles-mêmes, ce qui ne signifie pas qu'elle soit acceptée[1]. Les services de sécurité ont tendance à externaliser ces tâches de balayage du trafic et de recueil des données. Les compagnies nationales de télécom et les fournisseurs d'accès à internet – qui sont souvent

1. En Arabie saoudite, 63 % des personnes interrogées se disent inquiètes de la surveillance d'internet en 2019, contre 44 % seulement en 2013 (« Media use in the Middle East, a Seven-Nation Survey », Northwestern University in Qatar, 2019, http://www.mideastmedia.org/survey/2019/uploads/file/NUQ_Media_Use_2019_WebVersion_FNL_051219%5B2%5D(1).pdf).

des extensions du secteur public – jouent un rôle important à cet égard. Cette surveillance peut être confiée intégralement au secteur privé. D'après le rapport du laboratoire Citizen Lab, plusieurs États du Golfe ont fait appel à la société israélienne CSO[2]. Enfin, l'externalisation du renseignement prend également des formes originales. L'Iran peut compter des groupes de « hackers patriotiques » qui conduisent des opérations illégales dans le domaine cyber[3]. Ces groupes conduisent des actions de surveillance, voire des actions offensives à l'intérieur et à l'extérieur de leur territoire, sans que la responsabilité du gouvernement soit engagée. De telles opérations sont fréquemment observées en marge des conflits armés, comme actuellement dans la guerre russo-ukrainiene[4]. L'Iran élabore une stratégie de « blanchiment de l'influence » qui repose sur une combinaison de supervision bureaucratique et d'action d'agents non officiels, en Iran et à l'étranger[5]. D'autres gouvernements (Autorité palestinienne, Syrie, Turquie) sous-traitent les actions cyber à des *proxies*, qui collectent du renseignement et conduisent des opérations offensives. Des hackers palestiniens ciblent les militaires israéliens, notamment *via* des sites de rencontre, afin de recueillir des informations confidentielles. Ainsi sous-traitées, ces opérations sont à la fois moins coûteuses et plus difficiles à attribuer[6].

Les entités gouvernementales qui collectent des données en masse fusionnent en général celles qui proviennent de sources ouvertes et celles qu'ils recueillent par leurs moyens propres

2. Arabie saoudite, Bahreïn, EAU et Maroc utiliseraient le logiciel Pegasus (Bill Marczak, John Scott-Railton, Sarah Mc Kune, Bahr Abdul Razzak, Ron Deibert, *Hide and Seek, Tracking NSO Group's Pegasus Spyware to Operations in 45 countries*, Research report 113, Université de Toronto, septembre 2018, p. 10).

3. Collin Anderson, Karim Sadjadpour, « Iran's Cyber Threat, Espionage, Sabotage and Revenge », Carnegie Endowment for International Peace, 2018.

4. Rafal Rohozinski, « The missing 'cybergeddon': what Ukraine can tell us about the future of cyber war », The Survival Editors'Blog, IISS, 9 mars 2022.

5. Pierre Pahlavi, « L'Iran : stratégie asymétrique et diplomatie de masse », dans Céline Marangé et Maud Quessard (dir.), *Les guerres de l'information à l'ère numérique*, Paris, PUF, 2021, p. 198.

6. Valentina von Finckenstein, « Cybersecurity in the Middle East and North Africa », Konrad Adenauer Foundation Lebanon Office, juillet 2019, p. 7.

(images de caméras de surveillance, fichiers administratifs, cadastre, rapports médicaux). Les gouvernements de la région ANMO accèdent aisément aux données personnelles détenues par les différentes administrations, contrairement au modèle européen dans lequel les fichiers sont bien cloisonnés. Par exemple, la carte d'identité jordanienne, qui est déployée depuis 2016, permet d'accéder aux données biométriques, d'état civil et à l'adresse d'un individu. Ultérieurement, elle permettra aussi au gouvernement d'avoir accès à sa sécurité sociale et ses activités électorales[7].

Dans l'espace ANMO, certains gouvernements conduisent eux-mêmes des opérations informationnelles, revendiquées ou non. Par exemple, les autorités émiriennes ont lancé des programmes d'ingénierie sociale visant à réduire la demande pour de l'emploi public. Anticipant la baisse des revenus du pétrole, elles cherchent à influencer la mentalité des jeunes en valorisant le secteur privé, la réussite professionnelle par le travail, la pensée critique[8]. D'autres formes d'ingénierie sociale sont conduites par plusieurs États de la région. Depuis les révolutions arabes, plusieurs gouvernements (Arabie, Égypte, Émirats, Iran, Turquie…) se sont dotés de moyens pour limiter l'impact des réseaux sociaux dans les mouvements de contestation[9]. Twitter et Facebook s'emploient à fermer les comptes liés de trop près aux gouvernements. En septembre 2019, Twitter a annoncé publiquement la fermeture de plusieurs milliers de comptes en Arabie, en Égypte et aux Émirats, en raison de « campagnes informationnelles soutenues par le gouvernement[10] ». Le gouver-

7. Marwa Fatafta et Dima Samaro, « Exposed and Exploited: Data Protection in the Middle East and North Africa », Accessnow, janvier 2021.

8. Abu Elias Sarker, Mohammed Habibur Rahman, « Social engineering and Emiratization in the United Arab Emirates », *Public Administration and Policy: an Asia-Pacific Journal*, 173, 4 juin 2020.

9. Jeffery Wilson, Ashley Hahn, « Twitter and Turkey: Social Media Surveillance at the Intersection of Corporate Ethics and International Policy », *Journal of Information Policy*, vol. 11, décembre 2021.

10. https://blog.twitter.com/en_us/topics/company/2019/info-ops-disclosure-data-september-2019.html.

nement saoudien aurait recruté des anciens employés de Twitter pour surveiller plus de 6 000 comptes d'utilisateurs critiques du royaume. Une plainte a été déposée au tribunal de San Francisco en 2019[11]. La crise de 2017 entre le Qatar et d'autres pays du Golfe a conduit à des affrontements dans la sphère informationnelle. Les gouvernements respectifs ont mandaté des sociétés privées d'investigation pour rechercher des informations destinées à compromettre la partie adverse. Ces éléments ont pu ensuite être exploités dans le cadre de campagnes informationnelles. Parallèlement, des « lanceurs d'alerte » ont créé des sites spécialisés pour exposer les informations recueillies et discréditer l'adversaire : *Qatarileaks* (fuites sur le Qatar) et *Global Leaks* (fuites sur l'Arabie).

Ainsi, le champ informationnel est utilisé par les gouvernements de la région ANMO pour agir sur l'opinion publique.

PLATEFORMES ET GÉANTS NUMÉRIQUES

Les géants mondiaux du numérique sont présents dans presque tous les pays de la région ANMO. En centralisant et organisant l'information circulant sur internet, ils sont les intermédiaires obligés des utilisateurs. À l'évidence, ils accélèrent la transformation numérique, qui bénéficie aux économies locales et aux usages du quotidien. En Israël par exemple, plusieurs compagnies technologiques globales (IBM, Google, SAP et Samsung) ont investi dans des centres de recherche, ce qui leur permet d'attirer des talents et de les faire progresser. Les plateformes globales s'implantent aussi dans les pays du Golfe les plus avancés. Google et Microsoft développent des centres de données (*data centers*) en Arabie saoudite et aux Émirats, tandis qu'Amazon en a ouvert trois à Bahreïn en 2019. Ces infrastructures sont essentielles pour soutenir la consommation numérique croissante.

11. Daisy Nguyen et Brian Melley, « Saudis recruited Twitter workers to spy on critics », Associated Press, 7 novembre 2019.

Les Saoudiens sont les plus gros consommateurs de vidéos sur YouTube au monde *per capita*[12].

Les géants du numérique ont aussi des stratégies de conquête, voire de domination, qui créent de nouvelles dépendances. Par leur capitalisation, leur accès aux données (utilisateurs et fournisseurs), leur importance dans la vie quotidienne (communication, moteurs de recherche, géolocalisation, réseaux sociaux, commerces), ces plateformes en nombre très réduit acquièrent un pouvoir économique, politique et technologique exorbitant[13]. Ils imposent de nouveaux modèles de consommation, orientent l'activité économique et la recherche, et influencent les législations par leurs stratégies de lobbying.

De leur côté, des acteurs chinois occupent une place croissante en région ANMO. Les plateformes Alibaba, Tencent et Baidu profitent des révolutions numériques, du succès des équipements Huawei dans la 5G, ainsi que d'une régulation encore incomplète, pour se développer au détriment des GAFAM. Huawei étend son emprise dans le domaine des infrastructures mais aussi dans celui de la formation : la société a établi plusieurs centres de recherche dans le Golfe[14], sponsorise des salons internationaux qui s'y déroulent, tels Gitex, Word Cyber Security Summit, AI Everything ou SAMENA leaders.

Géants technologiques américains et chinois poussent leurs pions jusqu'aux limites de leurs zones d'influence respectives. En Iran, les autorités cherchent à s'opposer à l'emprise des GAFAM. Elles limitent l'accès aux réseaux sociaux qu'elles accusent de propager la contestation interne. Facebook, Twitter, YouTube et d'autres sont régulièrement interdits par les fournisseurs

12. Sara Hamdan, Angela Hundal, « Getting to know YouTube's biggest Middle Eastern audience: Millennials », Marketing Strategies, mars 2019, https://www.thinkwithgoogle.com/intl/en-145/marketing-strategies/video/getting-know-youtubes-biggest-middle-eastern-audience-millennials/.

13. Clara Hendrickson et William Galston, « Big Tech Threats: Making Sense of the backlash against online platforms », Brookings, 28 mai 2019.

14. Deux centres de recherche (un en Arabie, un aux Émirats) sont spécialisés dans l'internet des objets. Un autre, créé à Oman, sera hébergé au sein de l'opérateur Omantel et proposera des formations à l'IA et à la 5G.

d'accès. Les pays du Golfe sont à l'intersection des influences occidentales et orientales. Les équipements chinois liés à la 5G s'y déploient rapidement, sauf dans les secteurs sensibles, encore monopolisés par les Américains. Toutefois, dans certains ministères, l'incompatibilité entre équipements chinois et logiciels Microsoft provoque des *bugs* symboliques des frictions géopolitiques[15].

À l'international, les gouvernements de la zone ANMO risquent de se retrouver tiraillés entre les puissances chinoise et américaine, chacune cherchant à imposer ses équipements, ses normes et sa législation. La région ANMO risque de servir de terrain d'affrontement pour le contrôle des marchés stratégiques du futur.

SOCIÉTÉS PRIVÉES SPÉCIALISÉES DANS LA RECHERCHE ET L'INVESTIGATION

La zone ANMO intéresse un nombre croissant de sociétés privées spécialisées dans l'analyse de données, pour différents usages parmi ceux présentés dans la première partie. Certaines d'entre elles conduisent des activités de recherche et d'investigation, pour des gouvernements ou pour des clients privés. Elles peuvent être classées en fonction de la sensibilité de leurs activités de recherche.

Parmi les sociétés qui font des recherches sur le terrain, celles qui opèrent au profit des organisations internationales (notamment les agences de l'ONU) et des États eux-mêmes, disposent d'une assez grande latitude. De même, celles qui sont liées aux bailleurs institutionnels, dans le domaine de l'urgence, de l'éducation et du développement, sont en général bien acceptées des gouvernements[16]. Plutôt que des investigations à proprement parler, ces sociétés réalisent des études d'impact, des audits ou des

15. Entretien avec un fonctionnaire koweïtien.

16. Christelle Perrin, « La nature de la relation entre gouvernement et associations : le rôle de la confiance », *Revue interdisciplinaire management, homme et entreprise*, 2:6, 2013, p. 92-105.

enquêtes. S'appuyant sur la technologie, elles utilisent une très grande variété de méthodes de collecte de données pour observer, compter, mesurer, identifier, déterminer des localisations. Elles peuvent avoir accès à des données mises à disposition par les gouvernements. Toutefois, beaucoup préfèrent opérer à distance pour optimiser la sécurité, le confort de travail et les coûts. Cependant, quand les capteurs ne sont pas opérants, ou que les analyses présentent des incohérences, la collecte de données doit être complétée par un travail de terrain[17]. L'interaction avec la population, souvent sous la forme d'interviews, enrichit considérablement l'analyse. Elle permet de confirmer (ou d'infirmer) une hypothèse, de nuancer une analyse à partir d'un paramètre dont la pertinence apparaît brusquement[18].

Parmi les entreprises françaises appartenant à cette catégorie technique, Preligens (ex-Earthcube) travaille pour des clients étatiques, Masae Analytics pour des agences internationales et des ONG. Ces sociétés conduisent une grande partie de leur activité à distance. En plus, elles disposent aussi de relais locaux dans la zone ANMO (et en Afrique).

Les véritables sociétés d'investigation opèrent dans des domaines sensibles. Travaillant principalement au profit de clients privés (entreprises, cabinets d'avocats, compagnies d'assurances, cabinets en communication), elles proposent des études de marché (préalables à une commercialisation ou une implantation), des recherches sur une société ou sur une personne (évaluation de sa probité et de ses avoirs), un traçage des actifs financiers (notamment liés aux cryptomonnaies). Elles sont souvent sollicitées pour évaluer la fiabilité d'un potentiel partenaire en affaires ou pour identifier des vulnérabilités. Parfois, elles le sont pour alimenter une procédure devant les tribunaux.

17. Par exemple, lorsque des masques de végétation rendent inexploitables les photos prises du ciel.

18. Dans une étude sur les dommages occasionnés par la guerre dans la vallée de Ninive, seule une enquête de terrain avait permis d'établir un lien entre la proximité de la zone des combats et la destruction des oliviers (entretiens avec des responsables de MASAE).

Officiellement, elles s'appuient sur des sources d'information relevant du domaine public : presse, actes administratifs et judiciaires, registres de sociétés, voire banques de données de brevets[19]. Toutefois, en raison du manque de ressources disponibles en ligne, ces sociétés sont amenées à rechercher l'information de manière parfois offensive. Elles s'appuient sur des avocats qui ont accès aux greffes des tribunaux et sur des agents qui ont leurs entrées dans les administrations. Certaines utilisent même des méthodes intrusives pour obtenir des informations très sensibles (corruption, effraction…). Une partie de ces sociétés est également spécialisée dans le domaine cyber[20].

Les grandes sociétés opérant dans la région ANMO pour ce type d'investigation sont internationales, les plus emblématiques étant américaines (Kroll Inc., FTI Consulting, Verisk Maplecroft, Stratfor) et britanniques (Control Risk, Global Risks Insights, IHS). De nombreux cabinets anglo-saxons opèrent dans les champs couverts par la législation de leurs pays d'origine et qui confère aux juges des prérogatives extraterritoriales : lutte contre la corruption, le blanchiment d'argent, le crime organisé, ou encore le terrorisme[21]. La France compte plusieurs sociétés de renseignement d'affaires opérant en région ANMO : l'ADIT, Avisa, Amarante.

Ces cabinets emploient volontiers des spécialistes ayant servi dans les services de renseignement, l'armée ou la police. Ce recrutement leur permet d'entretenir des liens avec les services de sécurité nationaux, mais aussi d'appliquer souvent des méthodes similaires. Ils recourent à des plans de recherche assez normés. Ils ont accès à des bases de données (commerciales, juridiques, presse) publiques ou payantes. Surtout, ils utilisent des outils de recherche sur les différentes strates du web et tout

19. Entretien avec Joël Rey, expert de l'OSINT.

20. Entretien avec un expert en intelligence économique basé dans la zone ANMO.

21. Les plus connues étant la loi américaine *Foreign Corrupt Practice Act* (FCPA) et la loi britannique *United Kingdom Bribery Act* (UKBA). Rapport d'information de l'Assemblée nationale sur l'extraterritorialité de la législation américaine du 5 octobre 2016.

particulièrement sur les réseaux sociaux. Ils utilisent en général des VPN et des outils de recherche discrets, tels les moteurs de recherche Tor. Certains de ces cabinets ne se limitent pas à un travail de recherche, mais conduisent également des opérations d'influence (actions en réputation par exemple).

Les plus grandes sociétés de renseignement d'affaires sont établies en dehors de la région ANMO, aux États-Unis et en Europe. En étant implantées dans les grandes métropoles comme New York, Londres, Paris ou Genève, elles ont un contact plus facile avec leurs clients internationaux (des « grands comptes »). En outre, en opérant à distance, elles ne sont pas soumises aux pressions qui pourraient être exercées localement.

Toutefois, ce travail à distance s'avère insuffisant si le client recherche une véritable étude de terrain, comportant des références précises (noms, coordonnées, adresses, photos). Les meilleurs outils technologiques ne remplacent pas la compréhension culturelle ni le témoignage d'acteurs locaux. Cette exigence impose aux sociétés de disposer de relais au plus près de la zone de recherche. Ainsi, pour conduire une mission ponctuelle dans un pays tiers, une entreprise peut faire appel à un consultant ou agent local, qui sera rémunéré au service rendu. Si une présence plus durable se révèle nécessaire, elle peut se faire représenter par une société locale. Cette formule représente un coût moindre que d'ouvrir des bureaux dans le pays-cible. Cette option se justifie en cas d'opportunités d'affaires importantes, ou s'il est indispensable d'approcher les clients locaux : démarches commerciales, définition du besoin, accompagnement pendant la durée du service. L'ouverture d'un bureau offre aussi l'accès à des sources d'information inaccessibles à distance et une plus grande facilité à obtenir les autorisations légales et réglementaires pour opérer sur le terrain.

À l'inverse, une implantation locale expose au contrôle des autorités. Dans de très nombreux pays ANMO, une société qui s'implante ne peut le faire qu'en créant une société de droit local, ou en s'associant avec un partenaire local. Dans la région du Golfe, un sponsor (*kafil*) est en général obligatoire. Or, dans un

domaine sensible comme celui du cyber ou de l'analyse de données, ce sponsor sera nécessairement lié au gouvernement[22].

La cartographie des sociétés d'investigation dans la région ANMO reproduit assez fidèlement l'activité économique. La plupart des acteurs sont établis dans les grands centres d'affaires, qui sont souvent les capitales des pays concernés : Abou Dhabi, Bahreïn, Beyrouth, Casablanca, Dubaï, Tel-Aviv, Riyad.

Israël compte de nombreuses sociétés spécialisées dans l'investigation. Le pays a beaucoup d'avance dans ce domaine car ses services de renseignement ont développé cette approche dès les années 2000, en particulier au sein de l'unité 8200. Cette unité spécialisée dans le renseignement technique et les opérations cyber est un gigantesque centre de formation permanent. Parmi les milliers de jeunes qui en sortent chaque année, très aguerris dans le domaine du renseignement d'origine cyber (entre autres techniques), beaucoup poursuivent cette activité une fois revenus à la vie civile. Une partie d'entre eux ont créé de petites sociétés à forte composante technologique, travaillant sur des applications civiles ou militaires.

Global Osint, basée à Tel-Aviv, opère pour le compte de sociétés privées et de gouvernements. Elle compte une branche spécialisée pour le Moyen-Orient, MENA OSINT, qui travaille sur des sources arabes, turques et iraniennes grâce à la maîtrise de ces langues par ses employés[23]. Global OSINT est dirigée par Nachum Shiloh, qui indique être passé par les services israéliens avant de créer cette entreprise en 2010. Shiloh est également professeur à l'université de Tel-Aviv.

La société NSO a été créée en 2010 par d'anciens membres de l'unité 8200. Elle développe des outils de surveillance destinés à « prévenir le terrorisme et la criminalité », mais aussi à « aider les gouvernements à maintenir la santé publique »[24]. Selon ses détracteurs, ces outils seraient utilisés pour surveiller les journalistes et les opposants, ou même pour espionner des

22. Entretien avec François Delerue, chercheur à l'IRSEM (2017-2021).
23. https://www.globalosint.com/MENA-OSINT-1.html.
24. https://www.nsogroup.com/.

gouvernements. Le logiciel Pegasus, best-seller de CSO, aurait été utilisé pour écouter des milliers de personnalités dans plus de 40 pays. Selon le laboratoire Citizen Lab, il aurait été vendu à plusieurs États du Golfe pour cibler des milliers de journalistes, avocats et opposants[25]. Ces révélations sont documentées par une enquête menée par un collectif de journalistes (Forbidden Stories), en juillet 2021[26].

Diagramme des possibilités offertes par le logiciel Pegasus (The Citizen Lab)

25. Bill Marczak, John Scott-Railton, Sarah Mc Kune, Bahr Abdul Razzak, Ron Deibert, *Hide and Seek, Tracking NSO Group's Pegasus Spyware to Operations in 45 countries*, *op. cit.*, p. 10.
26. Damien Leloup et Martin Untersinger, « "Projet Pegasus" : révélations sur un système mondial d'espionnage de téléphones », *Le Monde*, 18 juillet 2021.

Quelques sociétés sont implantées au **Liban**, où elles profitent d'un écosystème favorable : proximité de zones de crise, main-d'œuvre (ingénieurs, linguistes, informaticiens) qualifiée et bon marché, fiscalité avantageuse. Formellement, les sociétés implantées au Liban et opérant dans le domaine de la sécurité ne doivent employer que des citoyens libanais. Compte tenu de cette restriction, seuls un ou deux acteurs se partagent le marché, notamment Masri Group[27]. D'autres sociétés, qui emploient des consultants étrangers, doivent se limiter à l'investigation (analyse forensique) pour être autorisées. C'est le cas de Nigma, une société dirigée par Fabien Tabarly, un ancien militaire français passé par les forces spéciales. Elle propose une large gamme de prestations rendues possibles par l'analyse de données et l'OSINT[28].

La **région du Golfe** compte de nombreuses sociétés qui recourent à l'analyse de données. La plupart ont développé une petite capacité *big data* pour améliorer leur productivité dans leur activité principale, dans toutes sortes de secteurs (énergie, transport, santé…). Ils dédient quelques experts (*data scientists* ou analystes cyber) à cette tâche. Il existe aussi un nombre croissant d'entreprises spécialisées dans la science des données, qui opèrent dans le renseignement d'affaires, la sécurité ou le conseil. Elles trouvent dans le Golfe un écosystème favorable à cette activité (investissements, fiscalité, législation).

Les **EAU** comptent de nombreuses sociétés spécialisées dans la sécurité, l'investigation et la recherche. La société Electronic Identity Management and Security Solution gère le contrôle biométrique dans plusieurs aéroports. Elle est à la fois la filiale d'un groupe international, tout en étant très proche du ministère de l'Intérieur émirien. Quant Azimuth opère dans le renseignement d'affaires et dans la sécurité. Dark Matter est un acteur privé du cyber, qui travaille notamment pour le compte du gouvernement.

27. Cette société effectue principalement du renseignement d'affaires, https://www.masri.com.lb/.

28. *Blockchain forensics*, évaluation de risque, *due diligence*, etc. Nigma utilise les logiciels suivants : Liferaftinc.com, Echosec.net, Mediasonar.com, Skopenow.com.

Au **Koweït**, l'intelligence économique et l'investigation sont assez peu développées. Dans ce pays de dimension réduite, les hommes d'affaires s'appuient sur des relations de confiance, souvent familiales, plutôt que sur les services d'un cabinet de conseil. Les besoins en renseignement d'affaires sont moins importants qu'ailleurs, d'autant qu'une société étrangère n'a pas besoin de nouer un partenariat avec un partenaire local si elle veut s'implanter dans l'émirat.

L'**Arabie saoudite** constitue un terrain privilégié pour l'analyse de données car la population y est très jeune et extrêmement connectée[29]. De grandes sociétés étrangères y opèrent dans le domaine du renseignement d'affaires et de l'ingénierie sociale. Un écosystème national a émergé depuis les années 2000, à partir de sociétés de services informatiques fondées sur impulsion gouvernementale. Al-Elm Information Security Co s'est développée en proposant des services publics en ligne (visas, santé, régulation des véhicules et des permis de conduire)[30] et Qwaed Technologies à partir de services informatiques aux particuliers comme aux entreprises. Deux sociétés particulièrement proches du gouvernement opèrent dans le domaine de la cybersécurité. Technology Control Company a un positionnement très marqué dans les domaines de la sécurité et de l'investigation : surveillance (physique et numérique), recherche dans le domaine cyber, reconnaissance faciale, ingénierie sociale (sur Twitter)[31]. Elle aurait des contrats avec le ministère de l'Intérieur et les services de renseignement[32]. Saudi Information Technology Company a aussi été créée avec des capitaux publics et travaille pour le gouvernement. En résumé, la plupart des sociétés saoudiennes évoluant dans le domaine de l'analyse de données et, plus généralement, celles qui sont liées au cyber, ont des accointances avec le gouvernement. Bien qu'étant de droit privé, elles disposent

29. L'utilisation quotidienne d'internet est passée de 93 % à 99 % de 2013 à 2019 en Arabie (« Media use in the Middle East, a Seven-Nation Survey », Northwestern University in Qatar, 2019).

30. https://www.elm.sa/en/Pages/default.aspx.

31. https://www.tcc-ict.com/en/about/#.

32. *Intelligence online*, 861, 23 septembre 2020 et 872, 10 mars 2021.

de financements et de commandes publics. Surtout, elles sont dirigées par des personnes proches du pouvoir saoudien. Le contrôle est exercé, entre autres, par la National Cybersecurity Agency, créée en 2017.

Au **Qatar**, quelques sociétés se sont lancées sur le marché de l'analyse de données, en prévision de la Coupe du monde 2022, attirés par les budgets colossaux investis. Ces sociétés (en majorité anglo-saxonnes) opèrent essentiellement pour le gouvernement, dans des champs soigneusement définis par celui-ci.

L'**Iran** voit émerger quelques sociétés opérant dans le domaine cyber et dans celui des données. Comme dans les pays arabes du Golfe, l'activité est impulsée par l'État. Les services gouvernementaux investissent activement ce champ, tout en exerçant un contrôle sur les centres de recherche et les cabinets privés spécialisés.

Le Middle East Center of Data Science, basé à Téhéran, propose un service d'analyse de données stratégiques pour les entreprises (notamment du secteur bancaire), d'analyse de réputation[33].

La société IPSOS possède des bureaux dans la plupart des pays du Golfe. Elle conduit des enquêtes fondées à la fois sur des sondages et sur des sources ouvertes issues d'internet[34]. Elle produit des études très diverses en fonction des clients, publics ou privés : tendances de consommation, perceptions, prévisions économiques ou sociales.

Chypre valorise un positionnement géographique très favorable, à la croisée de l'Europe et du Moyen-Orient, pour attirer des acteurs technologiques recherchant une certaine permissivité. De nombreux ingénieurs arabes, israéliens et russes s'y sont installés. L'Institut d'innovation Pafos, établi en partenariat avec l'université d'Herzliya (Israël), sert de pépinière pour les start-up technologiques.

33. http://www.mecds.com/.

34. Son outil d'ingénierie sociale analyse 600 millions de sources dans 80 langues.

En comparaison des progrès observés au Proche et Moyen-Orient, l'analyse de données est peu répandue en **Afrique du Nord.** À Tunis, ces techniques ne sont pas utilisées par les tribunaux et ne sont pas connues de la plupart des avocats[35]. En Algérie, il y a peu d'espace pour l'investigation privée, compte tenu du contrôle gouvernemental très fort. D'ailleurs, les cursus cyber sont pratiquement inexistants à l'université. Casablanca se positionne comme un grand centre d'affaires à l'échelle du continent africain. Des sociétés d'intelligence économique, ainsi que de grands cabinets d'audit, s'y installent, mais le cyber et l'IA sont encore peu implantés[36].

En **Libye**, l'analyse de données est peu développée car l'information à haute valeur ajoutée (enjeux pétroliers et migratoires) ne circule pas sur les réseaux sociaux ou d'autres supports technologiques. Certains cabinets d'information stratégique travaillent pour le gouvernement, des ambassades, des compagnies pétrolières et des ONG. On citera deux cabinets, de taille réduite, mais bien informés : North Africa Consulting et Fezzan Consulting, Ces sociétés sont rarement libyennes et leurs sources sont essentiellement humaines[37].

PRESSE SPÉCIALISÉE

Les médias utilisent les données pour acquérir l'information à partir de traitements algorithmiques. Ceux-ci permettent de mieux connaître les attentes du public (veille des contenus diffusés et même prédiction de ce qui pourrait « faire le buzz ». Ils peuvent aussi diffuser des contenus automatiquement (« journalisme robotisé »).

Inversement, la presse spécialisée est utilisée comme source d'information par des acteurs de la connaissance et de l'investigation.

35. Entretien avec un avocat tunisien.

36. Accenture, Boston Consulting, Deloitte, Mc Kinsey (et d'autres) ont des bureaux à Casablanca. De là, ils couvrent parfois l'ensemble de la zone Afrique et Moyen-Orient.

37. Entretien avec un professionnel de la sécurité opérant en Libye.

Plusieurs journaux spécialisés dans la région ANMO utilisent leur réseau de journalistes d'investigation afin de conduire leurs enquêtes : *Africa Intelligence, Maghreb Confidentiel, Intelligence Online* (pages Moyen-Orient), *Middle East Business Intelligence*. En fonction de leur spécialisation et de leur fiabilité, ces publications crédibilisent les informations et les enquêtes produites. En 2015, l'hebdomadaire *Der Spiegel* a diffusé des documents exclusifs sur Haji Bakr, un stratège de l'État islamique, qui ont servi de références aux chercheurs et aux services de renseignement[38].

Les journalistes spécialisés dans la région ANMO sont en majorité basés dans la zone, mais certains sont actifs depuis Londres ou Paris.

THINK TANKS ET INSTITUTS DE RECHERCHE

La zone ANMO compte plus d'une centaine de think tanks et d'instituts de recherche. Ces centres sont souvent liés aux gouvernements ou à des universités. Ils travaillent principalement sur les politiques publiques[39]. Ils jouent parfois le rôle de relais d'influence, notamment dans le Golfe.

Ces organisations recourent de plus en plus à l'analyse de données. Beaucoup « ratissent » les innombrables sources d'internet pour en extraire l'information utile. La veille des réseaux sociaux, en particulier, permet d'objectiver des tendances. Les outils informatiques établissent des statistiques et des graphes à partir des contenus internet, bien plus facilement qu'à partir d'interviews et de questionnaires.

Gros consommateurs de données pour leurs études, ils appellent les acteurs publics et privés à les publier. Partisans de l'e-gouvernement et de la transparence, au même titre que

38. Christoph Reuter, « The Terror Strategist Secret File Reveal the Structure of Islamic State », *Der Spiegel*, 18 avril 2015.

39. Cent un centres de réflexion sont reconnus dans le classement *2020 Global Go Think Tank Index Report*, The Lauder Institute, University of Pennsylvania, janvier 2021, https://www.bruegel.org/wp-content/uploads/2021/01/2020-Global-Go-To-Think-Tank-Index-Report_Bruegel.pdf.

certaines ONG, ils sont donc des promoteurs des technologies de données, plutôt que de purs acteurs de cette discipline.

ORGANISATIONS NON GOUVERNEMENTALES (ONG) ET INTERGOUVERNEMENTALES

Les ONG ne sont pas non plus strictement des acteurs de la donnée, mais elles en font un usage croissant. Elles intègrent l'analyse de données parmi leurs outils opérationnels et d'analyse ce qui, en retour, participe au développement de cette technique. Elles ont volontiers recours à la donnée comme un élément de preuve, surtout si l'accès à l'information est compliqué.

À cet égard, on peut établir une distinction entre deux catégories d'ONG. Celles proches du pouvoir (souvent parapubliques, qui disposent de financements gouvernementaux et dont les responsables sont désignés par les autorités) ont accès aux informations dont elles ont besoin pour travailler. Elles ne suivent donc pas, en général, une démarche d'investigation. À l'opposé, les organisations plutôt critiques des pouvoirs en place comme Amnesty International, Human Rights Watch ou Reporters sans frontières, cherchent à documenter les tendances et les pratiques qu'elles dénoncent. Elles ont volontiers recours à des techniques d'OSINT pour enquêter sans prendre de risques inconsidérés.

Certaines ONG ont mené des enquêtes qui ont fait référence, comme ce rapport sur le programme d'interrogation extra-judiciaire de prisonniers conduit par la CIA, dans le cadre de la lutte contre le terrorisme[40]. Publié en 2006, il est le fruit d'un long travail de collecte, de recoupement et d'analyse de données ouvertes. Dans ce cas, la simple corrélation de diverses sources ouvertes (notamment de l'aviation civile internationale) a permis d'identifier des activités clandestines. Dans la région ANMO, de nombreuses ONG enquêtent dans le domaine des droits humains ; certaines, moins nombreuses, le font au nom de la bonne gouvernance, de la transparence financière ou de l'environnement.

40. https://www.amnesty.org/en/documents/pol30/003/2006/en/.

Les organisations intergouvernementales et agences des Nations unies recourent massivement aux données, dans un cadre opérationnel ou pour documenter des phénomènes. Les études et enquêtes qui en résultent s'apparentent à des travaux de recherche. L'UNODC conduit par exemple une étude annuelle sur le trafic d'armes illégales[41]. Elle s'appuie sur des questionnaires remplis par les États qui acceptent de le faire (seulement 5 ou 6 selon les années), mais aussi sur les données des douanes et par celles transmises par d'autres agences de l'ONU[42].

D'autres outils sont davantage appliqués et opérationnels. Le Programme alimentaire mondial (PAM) et la Haute Commission pour les réfugiés (HCR) ont recouru à une technologie du scan de l'iris dans un cadre humanitaire en Jordanie. Le système *Eyebank*, déployé en 2016 dans les camps de Zaatari et d'Azraq, permettait de savoir si un réfugié avait été dûment enregistré et s'il avait déjà perçu son quota alimentaire[43].

L'organisation de l'alimentation et de l'agriculture (FAO) met en place des outils gratuits et accessibles à tous pour le suivi des essaims de criquets et de sauterelles, qui provoquent des ravages dans toute la région ANMO – et plus largement, de l'Afrique de l'Ouest jusqu'au sous-continent indien. La FAO met à jour une base de données appelée *locust hub*, qui permet de visualiser la progression de ce fléau. Les données sont collectées *via* les gouvernements des pays affectés ainsi qu'à partir de contributions individuelles. La FAO appelle les particuliers à faire remonter les informations (localisation, photos, observations de terrain) au moyen d'une application qui s'installe sur les téléphones mobiles[44].

41. Elle produit un document annuellement, le *Global Study on Firearms Trafficking*, https://www.unodc.org/unodc/en/firearms-protocol/firearms-study.html.

42. D'après Max Menn, expert en prévention du crime et en justice criminelle (UNODC).

43. Entretien avec un Jordanien.

44. L'application eLocust fonctionne sur Android et sur IOS : https://apps.apple.com/us/app/elocust3m/id1510684948?ls=1.

À partir de ces données, rassemblées dans une base participative, l'intelligence artificielle prévoit les déplacements de ces nuées de criquets grâce aux outils intégrant paramètres météorologiques (vent, pression, température…) et données agronomiques. Ces prévisions peuvent réduire l'impact désastreux des criquets en les ciblant avant que leurs ailes ne leur permettent de se déplacer (jusqu'à 150 km par jour).

BLOGUEURS ET « JOURNALISTES-CITOYENS »

Dans les régions en guerre, ou dans celles où les journalistes sont réprimés par le pouvoir en place, les médias professionnels renoncent de plus en plus à envoyer des correspondants. Les contenus sont produits par les agences de presse, mais surtout par les journalistes-citoyens, en général des personnes vivant sur place, souvent jeunes, exerçant parfois un autre métier. Connaissant bien leur environnement, ils n'ont pas besoin d'un « fixeur » (accompagnateur de terrain).

Le développement d'internet et des plateformes de publication faciles d'usage ont favorisé la progression très rapide de cette nouvelle méthode de journalisme. À son tour, celle-ci a permis une démultiplication de la production de données en provenance du terrain, dans les années 2000 et surtout 2010. À cet égard, le conflit syrien a été un accélérateur du changement pour le reportage en zone de guerre. La Syrie s'est morcelée en une multitude de petites zones de conflits comme autant de territoires cloisonnés. Seuls pouvaient y accéder les personnes qui y vivaient et qui y combattaient. Par conséquent, la couverture du conflit a échappé aux médias traditionnels, au profit de milliers de contributeurs de terrain : simples observateurs ou belligérants. De fait, les principaux groupes rebelles avaient des comptes sur les réseaux sociaux. Ils communiquaient ouvertement sur leurs opérations militaires, pour revendiquer des victoires, donner leur opinion ou prendre des positions politiques[45]. Les contenus diffusés étaient la plupart du temps authentiques, mais devaient

45. Échange avec Charles Lister, chercheur au Carnegie Middle East Center.

être appréciés avec une distance critique. C'est ce qu'ont permis de faire les journalistes-citoyens, forts de leur connaissance du terrain et de leur fonctionnement en réseau collaboratif. Des sortes d'agences de presse participatives se sont constituées sur le terrain syrien, grâce aux téléphones portables et aux réseaux sociaux : Aleppo Media Center, Enabbaladi, Halab Today TV entre autres. Les publications, majoritairement en arabe, sont avant tout destinées au public syrien. Chaque membre peut signaler un événement dès qu'il se produit, publier les photos et informations dont il dispose, tandis que les autres sont invités à confirmer ou infirmer les faits présentés[46].

Ces journalistes-citoyens assument en général deux fonctions : « sources primaires » de renseignement, au profit de médias, associations ou ONG, quand ils se trouvent à proximité de l'événement ; mais aussi producteurs de contenu, à partir d'informations qu'ils collectent auprès de sources dont ils ont – en théorie – vérifié l'authenticité.

Certains journalistes d'investigation (professionnels et amateurs) se regroupent pour donner plus de puissance et de précision à leurs enquêtes, grâce à la combinaison des outils de recherche (en source ouverte), à la vérification des faits et à leurs publications. Souvent basés en Europe et en Amérique du Nord, ils concentrent une partie de leurs travaux sur les zones en crise, dont celles de l'espace ANMO. Bellingcat est un site web emblématique de l'investigation, qui utilise des méthodes professionnelles de plus en plus sophistiquées. Il a enquêté entre autres, sur la guerre en Syrie, au Yémen et sur l'explosion dans le port de Beyrouth (août 2020)[47]. Les grands médias et agences de presse internationales ont également intégré ces contenus en provenance du terrain, même s'ils leur accordent une place relative[48].

46. Nora Palandjian, *Syrian Citizen Journalist Narratives: Central to Conflict Documentation*, The Aleppo Project, décembre 2017.

47. https://www.bellingcat.com/.

48. Nora Palandjian (*Syrian Citizen Journalist Narratives, op. cit.*) explique que les grands médias sont toujours inquiets de publier des informations non corroborées.

Parmi les nombreux journalistes-citoyens spécialistes du Moyen-Orient, deux ont acquis une grande notoriété au cours des années 2010. Rami Abdul Rahman a fondé l'Observatoire syrien des droits de l'homme (OSDH), un média qui se veut indépendant et spécialisé dans le conflit syrien. Rami Abdul Rahman a documenté tout le conflit, et continue à le faire, depuis le Royaume-Uni, où il s'est installé en 2000. Il compense son éloignement du théâtre d'opération par sa connaissance de la Syrie, mais surtout par ses 200 correspondants[49]. Abdul Rahman estime que la force de son réseau réside dans la propension de ses membres à témoigner, et à le faire par messagerie instantanée. Il pense aussi que son approche du journalisme surpasse celle des médias traditionnels, dont le fonctionnement est trop bureaucratique. À l'opposé, lui intervient à toutes les étapes de la construction de l'information, ce qui lui permet d'établir des liens avec des événements antérieurs et de replacer les faits dans un contexte qu'il maîtrise. Son site internet est une source d'informations très prisée des analystes OSINT, qui investiguent à partir des contenus mis en ligne et qui font des retours critiques.

L'OSDH a toutefois ses propres biais. Abdul Rahman a été très critiqué pour gérer seul tout le circuit de l'information et la fiabilité de ses sources a été remise en cause. Dans la plupart des cas, l'Observatoire est alimenté par les victimes qui ont tendance à exagérer les faits ou à les présenter de manière partiale ou incomplète[50]. Dans une guerre civile, la victime d'hier peut facilement devenir le bourreau de demain[51].

Figure emblématique du journalisme-citoyen irakien, Omar Mohammed a commencé à tenir un blog à partir de l'occupation américaine de son pays mais c'est en 2014 qu'il est devenu très

49. Interview de Rami Abdul Rahman par Reuters, 8 décembre 2011, https://uk.reuters.com/article/uk-britain-syria/coventry-an-unlikely-home-to-prominent-syria-activist-idUKTRE7B71XG20111208.

50. Ignace Leverrier, « La crédibilité perdue de Rami Abdel-Rahman, directeur de l'OSDH », blog, *Le Monde*, 19 décembre 2014.

51. Lucas Raineri, « If victims become perpetrators – Factors contributing to vulnerability and resilience to violent extremism in the central Sahel », International Alert, Unieri, 2018.

connu. Alors que la ville de Mossoul – où il habitait – était sous le contrôle de l'État islamique, il a tenu un blog clandestin pour relater la vie quotidienne sous l'occupation jihadiste (« L'œil de Mossoul »). Au péril de sa vie, il a fourni des informations extrêmement précieuses au monde entier sur des sujets économiques, sociologiques, politiques et militaires. Pour recueillir ces informations, il s'est comporté comme un habitant adhérant aux thèses jihadistes, en empruntant les codes vestimentaires et les comportements. Aujourd'hui, il a quitté l'Irak pour vivre en Europe, où il est protégé par le statut de réfugié politique.

Au-delà de la Syrie, de nombreuses plateformes de journalistes-citoyens se sont créées dans la zone ANMO. Elles sont alimentées par de nombreux auteurs, mais comptent aussi des journalistes professionnels. Elles cultivent l'authenticité (remontées de terrain par les contributions d'activistes, de lanceurs d'alerte et de simples observateurs), la liberté d'expression (tendance à la critique des gouvernants ou des « puissants »), le droit à l'accès à l'information et aux documents publics (*open data*). On trouve de très nombreuses plateformes en Tunisie (*Nawaat*), en Égypte (*Rassd*, qui a pris une part importante dans la révolution de 2011), en Turquie (*VivaHiba*, une plateforme qui permet à tous ceux qui veulent publier des photos ou des articles de le faire) et même en dehors de la région (*Middle East Eye*, qui agrège divers contenus en provenance de 24 pays de la région). En Iran, la scène journalistique est très contrôlée. Les plateformes d'information et les blogueurs qui y sont hébergés sont en général complaisants envers le pouvoir, ce qui ne veut pas dire que l'information qu'ils diffusent est de mauvaise qualité[52].

L'écueil principal de ces plateformes réside dans le parti-pris de leurs correspondants. Ceux-ci sont souvent des militants plus que de véritables journalistes. Les techniques de vérification des faits (*fact-checking*) et de production collaborative (*crowdsourcing*) ne garantissent pas la neutralité de l'information. Elles sont

52. Les deux « blogueurs » suivants sont très suivis pour les questions militaires : https://irangeomil.blogspot.com/ et https://twitter.com/BabakTaghvaee1/status/1317971314758569985.

souvent coordonnées par un journaliste-citoyen à partir d'un réseau de personnes qui ont une sensibilité du même bord.

Ce manque de distance vis-à-vis de l'information se conjugue avec un mélange de genres : quand le reporter de terrain se retrouve aussi modérateur de contenu, on ne peut pas parler de recoupement de l'information.

BILAN : LA DONNÉE CONFÈRE DES ATOUTS SUPPLÉMENTAIRES CONSIDÉRABLES AUX ACTEURS DE L'INFORMATION

La majorité des acteurs étudiés dans cette partie ont simplement élargi leurs processus d'acquisition de l'information grâce à la technologie. En s'appropriant ces nouveaux outils, ils ont voulu gagner en volume de données, en vitesse (traitement automatisé), en fiabilité (sources redondantes et corroborées) et en sécurité (travail à distance).

Depuis les années 2010, assez peu d'acteurs sont apparus avec les nouvelles technologies de la connaissance. Seuls les journalistes-citoyens et les sociétés technologiques (globalisées type GAFAM ou opérant à l'échelle locale) sont de véritables nouveaux venus. Pour l'instant, la plupart des acteurs privés collectent et traitent de la donnée pour des usages liés à leur modèle économique (marketing, vente, santé, finance, logistique, énergie) et non pour l'information en tant que telle. Ils pourraient toutefois changer d'approche en découvrant le potentiel contenu dans ces données une fois traitées, et en décidant de les valoriser davantage. À leur tour, ces acteurs privés deviendraient des producteurs d'information, qu'ils utiliseraient ou revendraient.

Qu'ils soient anciens ou nouveaux, les producteurs de connaissance trouvent dans l'analyse de données la possibilité de s'éloigner physiquement de l'objet de recherche. Cette distance est particulièrement utile lorsqu'il s'agit de suivre une zone de crise. En plus de la sécurité qu'elle procure, elle offre davantage de confort et de neutralité par rapport aux protagonistes locaux.

En outre, les nouveaux outils technologiques modifient les rapports de force, dans le champ de la connaissance. Jusque-là,

l'information stratégique était très strictement contrôlée, et connue d'un petit nombre de dignitaires et de leurs proches. Désormais, c'est l'accès à la donnée, davantage que l'accès au pouvoir, qui rend possible la connaissance.

Toutefois, l'accès aux data n'est pas suffisant. Compte tenu de leur variété, toutes les données n'ont pas la même valeur. Outre la capacité d'extraire les pertinentes, puis de les traiter, la valeur de l'information repose *in fine* sur l'analyse. Un analyste sans expérience de terrain pourra peut-être devenir un expert en ingurgitant énormément de ressources documentaires, mais il ne pourra pas appréhender finement un environnement complexe en se fondant exclusivement sur la technologie. Une visualisation trop réductrice des données peut mener à l'erreur. Alors qu'il était en charge de la sécurisation de la région de Tal Afar (Irak) en 2005, le général McMaster avait banni la présentation Power Point, dont il estimait que, « combinée avec certains indicateurs fallacieux, [elle était un outil] vraiment dangereux[53] ». De son côté, le général McChrystal (commandant des troupes américaines et de l'OTAN en Afghanistan en 2009-2010) ne cessait de répéter à son état-major qu'il fallait s'imprégner de la culture locale pour comprendre l'ennemi, plutôt que de se fier à des indicateurs[54].

Si le renseignement américain a eu recours de manière excessive à la technologie, au cours des conflits irakien et afghan, c'est sans doute en réaction à deux échecs emblématiques survenus quelques années plus tôt : l'incapacité à prédire le 11-Septembre et l'évaluation erronée des armes de destruction massive en Irak. Ces deux erreurs ont été imputées – *a posteriori* – à un croisement insuffisant des sources, à une mauvaise analyse, mais aussi à un renseignement humain défaillant[55].

53. Tom Ricks, « Gen. Mattis warns our military can become overpowering but still irrelevant », *Foreign Policy*, 12 avril 2010.

54. Entretien avec le colonel François Dickes, qui a servi dans l'entourage du général McChrystal.

55. Laurence H. Silberman et Charles S. Robb, *The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction*, Report to the President of the United States, Washington DC, 31 mars 2005),

Cette oscillation du renseignement américain entre technologie et connaissance du terrain traduit la nécessité de conjuguer simultanément ces deux approches. Pour Van Puyvelde, le traitement humain reste indispensable pour « évaluer la pertinence des corrélations, des tendances et *patterns*[56] ». Les données quantitatives doivent être mises en perspective par l'analyse humaine, qui requiert notamment de distinguer les *data* pertinentes de celles qui s'apparentent au « bruit de fond ». Il convient en particulier de déterminer les critères appropriés de recueil, pour catégoriser les données recueillies.

Faute de bon paramétrage, on risque de recueillir des données qui n'apportent pas d'éléments de réponse aux questions posées. Ce processus requiert une connaissance fine du terrain, ce qui donne en principe un avantage aux acteurs traditionnels de l'information (services de renseignement, sociétés d'investigation, ONG et journalistes).

Les deux approches peuvent se compléter. Lorsqu'un acteur de l'information veut aller le plus vite possible pour littéralement « avaler » des quantités massives de données, il cherchera à mettre en place un traitement automatisé. Si au contraire, disposant de temps, il privilégie la compréhension large et nuancée d'un phénomène complexe, il fera plutôt appel à l'analyse humaine. La recherche de la performance et du raccourcissement des délais incitera sans doute les acteurs de l'information à combiner les deux approches : réaction aux alertes et aux signaux faibles tirés des données collectées automatiquement ; analyse culturelle et humaine pour donner du sens aux tendances observées.

p. 2 ; US Congress, *Intelligence Reform and Terrorism Prevention Act 2004*, *public law 108-458*, 17 décembre 2004.

56. Damien Van Puyvelde, Stephen Coulthart et Shahriar Hossain, « Beyond the buzzword », *op. cit.*

IV. LES GOUVERNEMENTS FACE AU DÉFI DE LA DONNÉE

La zone ANMO présente un bilan contrasté vis-à-vis des données (volonté de contrôle des autorités mais exposition à la surveillance numérique) tout en suscitant l'intérêt de nombreux acteurs de ce domaine. Compte tenu de la croissance exponentielle du volume de données produites, les gouvernements de la région devront prendre en compte de nouveaux défis, afin d'exploiter ces nouveaux gisements de valeur tout en protégeant leur souveraineté.

DÉFI DE LA GOUVERNANCE

Rares sont les pays de la zone ANMO qui ont élaboré des stratégies spécifiques concernant l'utilisation des données ou celle de l'IA. Certes, il existe des documents assez généraux qui s'intègrent dans les plans stratégiques, du type Vision 2030 (Arabie, Bahreïn) ou Koweït 2035. Ces plans mettent l'accent sur la transformation digitale et sur la création d'infrastructures dédiées. Les EAU sont les plus avancés du monde arabe. Ils ont été les premiers (et pour l'instant les seuls en ANMO) à publier une stratégie pour l'IA (octobre 2017)[1] et ont mis en place un écosystème national : agence de sécurité cyber, plan de réponse aux incidents cyber. La ville de Dubaï est un véritable laboratoire de l'innovation numérique dont le schéma directeur figure dans une *Smart Dubai Strategy*[2].

Dans la plupart des pays ANMO, les administrations et organes de régulation d'internet ne dépendent pas du Premier ministre (comme l'ANSSI en France), mais d'un ministère en

1. « Mohamed Bin Rashid, « Launches UAE Artificial Intelligence Strategy », Gulf News, 16 octobre 2017, https://gulfnews.com/news/uae/government/mohammad-bin-rashid-launches-uae-artificial-intelligence-strategy-1.2106998, archivé https://perma.cc/4MXE-ZL9W.
2. https://2021.smartdubai.ae/.

particulier, souvent chargé de sécurité et de défense. C'est le cas aussi bien en Iran (Centre national du cyberespace, relevant du ministère de l'Intérieur) qu'au Maroc (Défense nationale). Ce positionnement renforce la propension au cloisonnement, fréquemment observée entre les administrations en charge du cyber. En outre, les agences de sécurité ont tendance à utiliser leurs prérogatives dans le sens de la répression plutôt que dans celui de la régulation.

Plus généralement, la prise en compte des données comme réserve de développement et de croissance doit s'intégrer dans une stratégie plus vaste en matière de technologies de l'information et d'intelligence artificielle.

S'ils veulent tirer le meilleur parti des données de masse tout en se protégeant contre les usages illégaux, agressifs et abusifs des technologies en question, les gouvernements de la région ANMO devront améliorer leurs structures de gouvernance et de régulation. Ils doivent définir une politique pour les données (et pour le numérique en général), et la décliner dans les administrations et les entreprises. Imposer une réglementation à l'ensemble des acteurs ne sera pas aisé, notamment ceux du secteur de la défense et de la sécurité qui sont en général très indépendants. Les services de renseignement ont tendance, dans la zone ANMO comme ailleurs, à utiliser les possibilités offertes par les données pour surveiller des catégories de population toujours plus grandes plutôt que de conduire des enquêtes ciblées sur des individus. Dans des systèmes très centralisés, comme on en rencontre souvent en région ANMO, la surveillance de masse risque de donner des pouvoirs accrus à un petit nombre de personnes, d'autant que la collecte de données massive s'accompagne en général du recours croissant à l'IA.

Les questions de gouvernance ont aussi une dimension internationale. Le choix des technologies et des protocoles détermine celui des partenariats. Plusieurs pays de l'espace ANMO, pourtant très liés aux États-Unis pour les questions de défense et de sécurité, ont fait le choix de fournisseurs chinois pour les infrastructures associées à la 5G (Arabie, Égypte, Émirats, Koweït, Maroc, Qatar). La surveillance vidéo au Qatar et à Dubaï

est, pour une bonne partie, gérée par des opérateurs chinois[3]. La téléphonie, la surveillance et la « ville intelligente » sont des secteurs cruciaux dans lesquels la Chine pourrait imposer ses normes technologiques et avoir accès à des données stratégiques. Huawei a signé des partenariats avec la plupart des opérateurs locaux pour la 5G[4]. La compagnie a aussi été choisie pour de nombreux projets de villes intelligentes : Yanbu (Arabie), Msheireb Downtown à Doha (Qatar), Dubaï (Émirats). Plusieurs villes israéliennes sont jumelées avec des villes chinoises très avancées dans ce domaine[5].

Les autorités américaines s'inquiètent à la fois de l'intégrité de leurs systèmes d'information (potentiellement compromis par des matériels ou logiciels chinois) mais aussi de la loyauté de leurs alliés, tentés par la technologie chinoise. Elles ont élaboré le concept d'un « réseau propre » destiné à contrer l'influence chinoise dans le numérique[6]. Dans ce cadre, elles auraient démarché plusieurs gouvernements de la région afin que ceux-ci renoncent aux équipements Huawei pour équiper les administrations et les forces de sécurité[7]. Cette politique n'est pas toujours suivie, notamment par les acteurs privés et locaux (collectivités et villes) qui disposent d'une plus grande autonomie dans leurs choix technologiques[8].

Ces tensions illustrent l'interdépendance entre les questions de technologie, d'alliances et de gouvernance. Il est illusoire d'ambitionner une stratégie nationale numérique sans disposer des ressources et des compétences correspondantes.

3. Entretien avec un ingénieur basé au Qatar.

4. Omantel et Ooredoo à Oman ; Viva, Zain, STC et Ooredoo au Koweït ; Viva à Bahreïn ; STC et Mobily en Arabie saoudite ; Etisalat aux Émirats arabes unis.

5. Netanya, Ashdod et Rishon Lezion sont jumelées respectivement avec Xiamen, Wuhan et Tianjin.

6. US Department of State, the Clean Network : https://2017-2021.state.gov/the-clean-network/index.html.

7. Entretiens avec des responsables de sociétés technologiques.

8. Hiddai Segev, « Smart Cities with Chinese Characteristics », *Strategic Assessment*, 24:3, juillet 2021.

DÉFI DES COMPÉTENCES, DES RESSOURCES ET DE LA SOUVERAINETÉ

La question de la souveraineté numérique se pose tout particulièrement en termes de capacités techniques et de formation.

Les gouvernements doivent disposer d'infrastructures nationales, et tout particulièrement pour l'hébergement de leurs données sur leur territoire. Plusieurs États, dont Israël, les Émirats et le Qatar, ont décidé d'investir dans des centres de stockage et dans un cloud souverain, afin de protéger les données de leurs administrations, de leurs entreprises et de leurs citoyens. Dans certains pays du Golfe, les données souveraines sont hébergées dans des infrastructures publiques et bien protégées ; les centres de données (*data centers*) sont placés sous tutelle des administrations liées à la sécurité (ministère de l'Intérieur souvent), quand ils ne sont pas directement gérés par le gouvernement, comme à Abou Dhabi. En plus des efforts portés sur les infrastructures (fibre optique, 5G, digitalisation), les Émirats et l'Arabie ont investi *via* leurs fonds souverains. Le Fonds public saoudien et la compagnie d'investissement Mubadala (Abou Dhabi) ont acquis des participations dans des sociétés technologiques indiennes (Jio Plateforms) et américaines (Uber entre autres)[9].

L'Iran a mis en place une architecture très autonome dès les débuts de l'expansion d'internet. Le développement d'infrastructures conditionne la question de la souveraineté, car les pays ANMO les plus avancés technologiquement vont produire des quantités considérables de *data* dans les années à venir. Les utilisateurs auront besoin de réseaux, de systèmes d'information et de serveurs aux capacités équivalentes. S'ils ne parviennent pas à les héberger dans des centres nationaux, ils seront obligés de le faire en dehors de leur territoire, exposant ainsi leur intégrité. On sait que le *Patriot Act* autorise les services de renseignement américains à accéder aux données stockées dans les serveurs des sociétés américaines (y compris hors du territoire américain),

9. Entretien avec un ingénieur réseaux opérant au Moyen-Orient.

au nom de la lutte contre le terrorisme. La législation chinoise donne aussi des pouvoirs exorbitants aux autorités nationales.

La souveraineté repose également sur l'existence de ressources humaines nationales qualifiées. En dehors des EAU et d'Israël, les pays de la zone ANMO ne comptent pas assez de nationaux pour armer l'ensemble des administrations, entreprises et universités dans les domaines technologiques. Beaucoup d'ingénieurs et d'experts en sécurité des systèmes d'information sont étrangers, tout particulièrement dans les pays du Golfe. Si les prestations technologiques sont effectuées par des sociétés étrangères, ou même par des sociétés nationales employant des experts étrangers, la souveraineté sur les données n'est pas garantie. De même, il est capital que les fonctionnaires qui assurent la maîtrise d'ouvrage des projets technologiques disposent du même niveau d'expertise que les ingénieurs du privé chargés de la mise en œuvre. Enfin, les services de renseignement nationaux doivent s'approprier ce nouveau domaine, avec tous les défis qu'il implique (équipements, méthodes, partage, etc.).

La région doit disposer de pôles de recherche dans les domaines technologiques, ce qui nécessite des investissements très importants et des filières de formation des jeunes. Il faut, pour former des experts de la donnée[10], développer les compétences informatiques et digitales à tous les niveaux du système éducatif. C'est en disposant d'experts bien formés, en nombre suffisant et avec des prétentions salariales raisonnables, que la région pourra développer des écosystèmes autonomes centrés sur les technologies de l'information et du cyber. La dynamique doit combiner impulsion gouvernementale (financement de la recherche et commandes publiques), développement de start-up et mise en place d'un cadre réglementaire approprié. Cet investissement a été engagé en Arabie, aux Émirats, au Qatar et dans certains autres pays. Les cursus universitaires en cybersécurité se développent dans le Golfe mais sont encore peu nombreux en Afrique du Nord.

10. Il existe de nombreuses spécialités telles que *data scientist*, architecte *big data*, développeur, administrateur.

L'enjeu des données met les gouvernants de la région sous forte tension. D'un côté, ils sont contraints de recourir aux sociétés technologiques pour remplir des missions régaliennes (police, justice, surveillance, renseignement…), comme l'a montré la crise sanitaire (recours à des applications anti-Covid, dont certaines ont été développées par les GAFAM). D'un autre, ils craignent d'abandonner leur monopole sur ces missions, notamment celles ayant trait à la sécurité nationale. Dans la plupart des pays ANMO, c'est le chef de l'État (président, roi ou prince) qui commande directement les forces de défense et de sécurité, souvent sans droit de regard du gouvernement ni du Parlement. Dans ces conditions, le souverain ne va pas à l'évidence prendre le risque de confier des missions sensibles à des entités indépendantes de son contrôle. Ainsi, les transferts vers le privé de missions régaliennes à connotation sécurité et renseignement sont souvent des externalisations biaisées[11]. Plutôt que de sous-traiter des projets sensibles à des entreprises réellement indépendantes, les souverains font appel à des sociétés technologiques dont les dirigeants sont proches du pouvoir et souvent dépendants de lui[12]. On observe ce phénomène dans les processus d'externalisation en Arabie, aux Émirats, en Égypte, en Israël et au Qatar. Toutefois, ces externalisations – même biaisées – ne sont pas toujours possibles. Lorsque le niveau d'expertise recherché dépasse les compétences nationales, les gouvernements n'ont d'autre choix que de faire appel à des sociétés étrangères, qui sont souvent des géants technologiques. Ceux-ci (aussi bien américains que chinois) ont tiré avantage de la crise sanitaire pour étendre leur influence et augmenter leurs profits de manière considérable[13].

De fait, la maîtrise des données est indissociable de la question de l'accès à la connaissance. Les gouvernements de l'espace ANMO ont tendance à contrôler étroitement l'information par

11. Entretien avec François Delerue, chercheur à l'IRSEM (2017-2021).

12. Cette dépendance repose sur plusieurs paramètres : agrément pour opérer, autorisation d'exporter, financements publics, désignation des dirigeants.

13. Les cinq GAFAM réunis ont vu leurs revenus augmenter de 20 % et leur capitalisation de 50 % pendant l'année 2020 (« How big tech got even bigger », *Wall Street Journal*, 6 février 2021).

des mécanismes de surveillance politique et sociale élaborés. Les échelons les plus élevés du pouvoir disposent traditionnellement d'un monopole exclusif sur les données stratégiques. L'apparition de nouveaux acteurs qui disposent de capacités technologiques leur donnant accès aux données sensibles vient bouleverser les équilibres internes. Lors des révolutions arabes, plusieurs régimes ont vacillé car ils ne maîtrisaient plus les flux d'information, notamment les appels à manifester sur Facebook et autres réseaux[14]. À l'inverse, les gouvernements les plus avancés technologiquement n'hésitent pas à censurer la diffusion de contenus potentiellement compromettants. Ainsi, après les attaques houthies contre Abou Dhabi en janvier 2022, les autorités émiriennes ont interdit la propagation de vidéos montrant les attaques par missiles ou les interceptions. Et encore, même la censure ne garantit pas la protection et le contrôle des données. Les gouvernants de la région redoutent le risque de fuites massives d'informations sensibles, type affaire Snowden.

Cette crainte de la dissidence informationnelle, ou des attaques cyber, a conduit certains gouvernements à s'adapter en agissant sur les réseaux. De fait, comme l'explique Maud Quessard, « un régime autoritaire peut protéger les flux informationnels bien plus facilement qu'une démocratie pluraliste[15] ». Le degré de contrôle exercé sur les flux de données est fortement corrélé avec le type de régime politique. Tenants stricts du contrôle, les Iraniens ont mis en place un système élaboré qui leur permet de fermer les portes d'entrée de leur réseau internet, en agissant à la fois sur les infrastructures physiques et sur la couche sémantique[16]. Les

14. David M. Faris, « La révolte en réseau : le printemps arabe et les médias sociaux », *Politique étrangère*, printemps 2012, IFRI, p. 99-109.

15. Maud Quessard dans l'émission *Géopolitique*, « Comment la révolution numérique redistribue les rapports entre États », RFI, 19 février 2021.

16. Ces deux systèmes autonomes sont l'Information Technology Company et la Telecommunication Infrastructure Company. Le flux de données peut être facilement interrompu, d'autant plus qu'il existe des protocoles de routage spécifiques, qui peuvent aussi être désactivés (Loqman Salamatian, Frédérick Douzet, Kevin Limonier, Kavé Salamatian, « The geopolitics behind the routes data travels: a case study of Iran », *Journal of Cybersecurity*, 7:1, 2021, p. 9).

autorités de Téhéran n'hésitent pas à couper internet à toute leur population, comme elles l'ont fait en 2019 pour mettre fin aux manifestations dans les grandes villes. Cette approche, inspirée du modèle chinois, a été également appliquée en Irak[17]. Toutefois, cette architecture n'est pas propice à la résilience, qui est elle-même une condition de croissance des entreprises et du dynamisme économique. Dans l'espace ANMO, Israël, les EAU et le Qatar ont développé des systèmes résilients[18]. Cette résilience n'est garantie que par des architectures internet complexes, servies par une diversité d'opérateurs, et ouvertes sur l'extérieur.

DÉFI DE LA PROTECTION DES DONNÉES PERSONNELLES

Les données fournies en utilisant des applications, des objets connectés ou en naviguant rendent possible une collecte massive de données personnelles, posant la question de leur protection. Dans une région où un niveau de contrôle étatique élevé est relativement accepté, les autorités sont tentées d'utiliser les données de leurs citoyens pour les surveiller ou pour orienter leurs décisions et leurs comportements. Par ailleurs, les données personnelles sont exposées au risque cyber, encore peu pris en compte.

Le *big data* procure également des perspectives gigantesques aux sociétés technologiques, notamment aux plus grandes d'entre elles. Le déploiement d'applications téléphoniques de traçage liées à la Covid-19 a fait connaître au grand public le potentiel de surveillance dont les gouvernements disposent. D'après Amnesty International, certaines de ces applications s'avèrent des « outils de surveillance de masse ». L'ONG estime que, parmi les trois applications les plus intrusives à l'échelle mondiale, deux ont été déployées en région ANMO[19]. À Bahreïn, au

17. Olivier Passot, « Les milices et la séquence de fin 2019 en Irak : un effet de levier stratégique », Note de recherche 101, IRSEM, 9 juin 2020, p. 20.

18. Michael Kende, *Middle East and North Africa Internet Infrastructure*, Internet Society, septembre 2020, .

19. Il s'agit de *BeAware Bahrain* (à Bahreïn) et de *Shlonik* (au Koweït) : https://www.amnesty.fr/actualites/covid-19-top-3-des-applications-de-tracage-les-plus-intrusives.

Koweït et au Qatar, les autorités ont croisé les données médicales et les informations personnelles (dont le numéro de téléphone, la localisation, le numéro d'état civil), ce qui leur garantissait des capacités de surveillance généralisée.

Au Moyen-Orient, la régulation du numérique est encore peu développée. Au Liban par exemple, la Constitution ne garantit pas explicitement le droit à la confidentialité des informations. La loi relative à la protection des données personnelles, adoptée en 2018, reste vague sur la notion de consentement à la collecte et au traitement des données[20]. Plus généralement, l'accès des individus à leurs propres données personnelles n'est presque jamais garanti dans la région ANMO. Les citoyens en font souvent l'expérience dans leurs démarches administratives, ou lorsqu'ils sont engagés dans des procédures auprès de tribunaux judiciaires ou administratifs[21].

Toutefois, la connaissance par le grand public des questions de données personnelles se diffuse rapidement. Les citoyens comprennent qu'il s'agit là d'un enjeu important. Ils sont prêts à accepter que les administrations et les entreprises utilisent leurs données à bon escient, à condition que la confiance soit établie.

Au Maghreb justement, les opinions publiques sont assez sensibles aux questions de vie privée. Les législations sont assez proches de celles qui prévalent en Europe, très protectrices des libertés, comme l'illustre le dispositif RGPD[22]. Deux États du Maghreb ont adopté des législations visant à protéger les données personnelles[23]. En Tunisie, une loi adoptée en 2018 reprend les principes généraux du RGPD et impose une obligation de

20. Loi N° 81 relative aux transactions électroniques et aux données personnelles (*Social Media Exchange*, octobre 2018).

21. Entretien avec un avocat travaillant au Moyen-Orient.

22. Le Règlement général sur la protection des données (RGPD), entré en application dans l'UE en 2018, encadre le traitement des données. Il existe peu de dispositifs aussi protecteurs dans le reste du monde.

23. Le Maroc et la Tunisie possèdent une législation et une autorité de protection des données personnelles. L'Algérie possède une loi mais pas d'autorité vouée à la protection des données personnelles, https://www.cnil.fr/fr/la-protection-des-donnees-dans-le-monde.

transparence à ceux qui utilisent les données. Le RGPD pourrait également inspirer les législations du Moyen-Orient, après celles du Maghreb.

La protection des données personnelles suppose une forte volonté politique et la mise en place d'un environnement juridique et administratif composé de trois éléments principaux : un cadre légal qui place les droits des citoyens au-dessus des intérêts économiques et de ceux des gouvernements ; l'existence d'une autorité indépendante, pour vérifier l'application de ce principe par le gouvernement et les entreprises ; une transparence de la part des pouvoirs publics dans l'usage des données. Tout ceci ne va pas de soi dans la zone ANMO, où d'autres modèles moins libéraux risquent de s'imposer. En s'inspirant du *Patriot Act* américain, plusieurs pays ont institué des dispositifs autorisant l'accès aux données personnelles par le gouvernement. Aux Émirats par exemple, le système du *name and shame* s'impose progressivement. Pendant la crise sanitaire, les photos des personnes contrevenant aux consignes de confinement ont été publiées dans les médias de Dubaï.

Par ailleurs, la protection des données personnelles nécessite des investissements importants en cybersécurité. La digitalisation a conduit à une augmentation des attaques informatiques, notamment dans les pays du Golfe. En réaction, plusieurs d'entre eux ont mis en place des stratégies cyber et des structures de sécurité informatique[24].

BILAN DES DÉFIS DU POINT DE VUE DES GOUVERNEMENTS

Les technologies liées aux données représentent d'immenses défis pour les classes dirigeantes de la région ANMO. Celles-ci seront de plus en plus exposées à des remises en question profondes de leurs modèles de gouvernance. Les États les plus riches et les plus avancés parviendront à s'adapter, en définissant des

24. Stratégie cyber au Qatar et aux EAU, structures de cybersécurité à Bahreïn, aux EAU, au Koweït.

stratégies nationales et en investissant dans la formation, les infrastructures et le cadre juridique. C'est le choix qui a été fait par plusieurs gouvernements du Golfe, qui appréhendent les technologies liées aux données comme un axe de diversification des économies en même temps qu'un outil de contrôle des populations.

Pour ce petit groupe d'États, la pandémie de Covid-19 a sans doute servi de banc d'essai et d'accélérateur dans la mise en place d'une forme de gouvernance technologique. Les Émirats, en particulier, ont délibérément fait le choix de l'IA pour le contrôle sanitaire, policier et social. Situés sur des territoires aux dimensions modestes, s'appuyant sur des infrastructures très modernes, dirigées par des princes au fait des enjeux technologiques, Abou Dhabi et Dubaï disposent d'atouts très favorables à cette forme de gouvernance. La plupart des autres États ne bénéficient pas de cet écosystème. Ils seront contraints de dépenser beaucoup, en technologie ou en dérive autocratique, s'ils veulent contrôler les données émises par leur population. S'ils n'investissent pas assez dans ces nouveaux champs, ils seront contraints d'abandonner des parts de souveraineté au profit d'acteurs désireux d'accroître leurs profits et leur puissance.

Ce contrôle devrait rester possible pour des acteurs non étatiques, dans des territoires circonscrits (zones enclavées ou déserts numériques) et pour des entités imposant une régulation numérique stricte (régime iranien, organisations militaires type PKK ou Hezbollah). La coupure pure et simple d'internet et des réseaux mobiles par les gouvernements (comme en Égypte au moment de la révolution de 2011, ou en Iran à intervalles réguliers) n'est certes pas compatible avec les principes démocratiques auxquels aspirent les peuples de la région, mais il est probable que certains gouvernements soient tentés par le modèle chinois de surveillance, rendu possible par les masses de données et l'IA. Plusieurs États du Golfe ont avancé dans cette direction à la faveur de la crise sanitaire[25].

25. James Shires, *The Implementation of Digital Surveillance Infrastructures in the Gulf, Digital Activism and Authoritarian Adaptation in the Middle East*, POMEPS Studies, août 2021.

En perdant leur monopole sur l'information sensible (notamment celui exercé jusque-là par leurs services de renseignement) les gouvernements vont être régulièrement exposés à la contestation de leur autorité. L'assassinat du journaliste Jamal Kashoggi par un commando saoudien dans le consulat d'Istanbul a été couvert et documenté par des journaux turcs, en s'appuyant principalement sur des images de vidéosurveillance[26]. Faute de maîtriser les données émises, les Saoudiens se sont retrouvés sur la défensive. Ce pouvoir égalisateur que confère la donnée (un citoyen bien formé peut en savoir autant qu'un dirigeant) a tendance à modifier les rapports de force politiques. À l'international, les gouvernements de la zone ANMO pourraient se retrouver tiraillés entre les puissances chinoise et américaine, chacune cherchant à imposer ses équipements, sa législation et ses normes. S'ils ne parviennent pas à un niveau suffisant de maîtrise technologique, leurs territoires risquent de servir de théâtres d'affrontement pour le contrôle des marchés stratégiques du futur (télécom, villes intelligentes, identité, santé).

26. J. Khashoggi a été assassiné le 2 octobre 2018 au consulat d'Arabie saoudite à Istanbul. Diverses images et données de sources diverses (vidéosurveillance, montre connectée, etc.) ont été diffusées dans les jours qui suivaient dans la presse turque.

CONCLUSION

Le recours aux données se développe massivement dans toute la région ANMO, pour de nombreux usages, notamment celui de l'accès aux informations stratégiques et réservées. Cette tendance va encore s'intensifier, portée par les innovations (5G, internet des objets, IA, robotique) et par l'engouement du public. La région ANMO sera particulièrement impactée en raison de son exposition numérique (digitalisation croissante et régulation encore restreinte). En outre, son positionnement géopolitique, à la croisée des influences américaine et chinoise, la prédispose à servir de terrain d'affrontement entre les deux puissances dominantes en matière de données et de technologie.

Ces technologies devraient permettre de contourner de nombreuses barrières à l'information, caractéristiques de la région ANMO : le contrôle politique et social, encore puissant aujourd'hui, ne suffira pourtant pas à endiguer la submersion digitale ; le niveau de danger prévalant dans les zones de crise sera relativisé par les possibilités de suivi à distance ; les données sensibles seront plus difficiles à protéger.

Les gouvernements de la région ANMO verront probablement se multiplier leurs capacités à surveiller, à espionner et à manipuler l'information ; toutefois, ils perdront leur monopole dans ce domaine, l'information étant devenue accessible à tous.

L'exposition numérique croissante va permettre à des acteurs toujours plus nombreux d'accéder à des informations à haute valeur. Médias et entreprises vont incorporer des méthodes innovantes pour accéder plus vite et plus largement aux données, pour les analyser et pour diffuser l'information. Parmi tous ces nouveaux acteurs, ce sont les géants technologiques qui vont concurrencer le plus fortement les services de renseignement. Les nouveaux entrants sur le marché de la connaissance, ayant accès à des données (brutes ou raffinées) à haute valeur, seront tentés de les utiliser par eux-mêmes ou de les monnayer. Certains évolueront dans une zone grise,

d'autres iront vers des pratiques illégales. Dans un environnement insuffisamment régulé, les manœuvres informationnelles et les manipulations (de type *hack and leak*[1] par exemple) risquent de se multiplier.

Les pratiques de surveillance et d'espionnage, mises en œuvre efficacement par de nombreux acteurs publics et privés, vont impacter le champ des libertés publiques et des droits individuels. Il est probable que les démocraties de l'espace ANMO seront atteintes aussi fortement que les régimes autoritaires. De nouvelles régulations se mettront en place, en fonction du niveau d'indépendance nationale par rapport aux grandes puissances numériques et du niveau de maîtrise technologique.

Les données – même si elles ne sont pas synonymes de connaissance – sont désormais à la portée de ceux qui maîtrisent les technologies, et non plus nécessairement de ceux qui sont proches du pouvoir ou qui possèdent le « droit d'en connaître ». Ce transfert de prérogatives du politique vers le technologique risque d'avoir des conséquences importantes en matière de gouvernance. Certains gouvernements de la zone ANMO risquent de se trouver fragilisés, voire marginalisés, alors que de nouveaux modes de transaction entre individus (type *blockchain*) se développent rapidement.

Les services de renseignement extérieurs opérant dans l'espace ANMO voient s'ouvrir des perspectives illimitées liées aux données en masse. Couplé à l'IA, le traitement de ces données garantit des performances beaucoup plus élevées, notamment dans les tâches de surveillance à grande échelle, ou celles qui nécessitent un temps de réaction très bref. Les services doivent adapter leurs outils et leurs méthodes pour automatiser certains de leurs processus opérationnels et pour déléguer une partie de la décision à l'IA. Dans un contexte de données abondantes et facilement accessibles, ce n'est pas leur

1. L'opération consiste à attaquer un système informatique pour se procurer des informations sensibles puis à les faire fuiter sur des sites spécialisés ou des réseaux sociaux.

quantité qui fera la différence, mais plutôt l'identification des indicateurs pertinents, et la capacité à collecter (et traiter) des données correspondantes. Cette capacité à discriminer les bons paramètres repose précisément sur une connaissance approfondie de la zone ANMO et, au moins en partie, sur l'analyse humaine[2]. Francis Beau insiste sur la notion de sens à donner aux données, afin qu'elles deviennent une connaissance explicite assimilable par un cerveau humain[3]. Autrement dit, les acteurs traditionnels conserveront toute leur place sur le marché de la connaissance.

Un espace ANMO « mis en données » offrira des gains de productivité considérables à qui recherchera la vitesse de réaction (systèmes de veille et d'alerte), la fusion de données multisources, les corrélations entre variables de recherche, etc. Toutefois, les technologies liées aux données sont surtout efficaces pour appréhender des situations binaires ou pour répondre à un besoin d'instantanéité. Lorsqu'on a affaire à des environnements complexes, elles sont moins pertinentes et peuvent même nous conduire à des conclusions simplificatrices[4]. En outre, le recours aux données ne fonctionne que s'il existe une interface numérique. Or, les systèmes de gouvernance très centralisés et attachés au secret (régimes oligarchiques, théocraties, sociétés familiales, groupes armés non étatiques), bien représentés dans l'espace ANMO, sont par principe réfractaires à la numérisation.

En matière d'anticipation, ces technologies doivent encore démontrer leur pertinence. L'usage des données est moins fiable dans une zone fréquemment soumise à des chocs et des « surprises stratégiques », et où la décision est souvent le fait du prince. Si les informations cruciales sont détenues dans le cerveau d'une ou de quelques personnes, la collecte de données quantitatives restera insuffisante pour accéder à la connaissance.

2. Entretien avec Reynaud Theunens, chef JMAC (*joint mission analysis centre*) au sein de l'ONU.

3. Francis Beau, « Le renseignement au prisme des sciences de l'information », thèse, Université de Valenciennes et du Hainaut-Cambresis, 2019, p. 268.

4. Martin Waehlisch, « How Dashboards could destroy peace – and how to prevent it », Futuring Peace, 20 mars 2021.

Cette singularité de l'espace ANMO rend toujours pertinente l'approche traditionnelle, tant le « terrain humain est difficile à modéliser[5] » à partir de données quantitatives et de modèles mathématiques.

5. Jean-Christophe Noël, *Intelligence artificielle : vers une nouvelle révolution militaire ?*, Études de l'IFRI, Focus stratégique 84, octobre 2018, p. 51.

ÉTUDE – n° 98

COMPRENDRE LE MOYEN-ORIENT PAR LA DONNÉE

TECHNOLOGIES NUMÉRIQUES ET ACQUISITION DE LA CONNAISSANCE DANS LA RÉGION AFRIQUE DU NORD / MOYEN-ORIENT

COL Olivier Passot

Les technologies liées au recueil et au traitement de la donnée ouvrent des perspectives considérables au regard de la connaissance et du renseignement, y compris dans un environnement peu perméable. Peuvent-elles permettre de décrypter plus facilement la région Afrique du Nord / Moyen-Orient (ANMO), souvent considérée comme compliquée dans l'imaginaire occidental ?
Cet espace présente une exposition contrastée à la donnée : d'un côté, la collecte est limitée par de multiples barrières (contrôle politique et social, insécurité, codes culturels) ; de l'autre, les individus sont de plus en plus exposés à la surveillance numérique en raison d'une régulation encore faible tandis que les comportements se digitalisent très vite. De fait, des acteurs publics et privés toujours plus nombreux collectent et analysent des *data* pour informer, investiguer et tracer, transformant le terrain de la connaissance en un espace concurrentiel. Si ces technologies offrent des opportunités à certains gouvernements de la région ANMO, dans l'exercice de missions régaliennes, elles représentent d'importants défis pour la majorité d'entre eux. L'acquisition des compétences, le contrôle des données et de la souveraineté nécessiteront des investissements très importants. Les États qui n'y parviendront pas risquent d'être concurrencés par les nouveaux acteurs de la donnée.

IRSEM, École militaire
1, place Joffre, case 38 - 75700 Paris SP 07
irsem.fr

IRSEM
INSTITUT DE RECHERCHE STRATÉGIQUE DE L'ÉCOLE MILITAIRE